FLHSMV
FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

# MEMORANDUM OF UNDERSTANDING
# FOR DRIVER'S LICENSE AND/OR MOTOR VEHICLE RECORD DATA EXCHANGE

This Memorandum of Understanding (MOU) is made and entered into by and between City of Fort Lauderdale, hereinafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereinafter referred to as the Providing Agency, collectively referred to as the Parties.

## I. Purpose

The Providing Agency is a government entity whose primary duties include issuance of motor vehicle and driver licenses, registration and titling of motor vehicles, and enforcement of all laws governing traffic, travel, and public safety upon Florida's public highways.

In carrying out its statutorily mandated duties and responsibilities, the Providing Agency collects and maintains personal information that identifies individuals. Based upon the nature of this information, the Providing Agency is subject to the disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (hereinafter "DPPA"), Sections 119.0712(2) and 501.171, Florida Statutes, and other statutory provisions.

The Requesting Party is a government or private entity operating under the laws and authority of the state of Florida and/or operating under Federal laws and is requesting personal information and declares that it is qualified to obtain personal information under the exception number(s), listed in Attachment I, authorized by DPPA.

This MOU is entered into for the purpose of establishing the conditions and limitations under which the Providing Agency agrees to provide electronic access to Driver License and Motor Vehicle information to the Requesting Party. The type of data requested and the statutory fees, if applicable, are agreed to by both parties as indicated in Attachment II.

The Requesting Party is receiving ○ 9-digit ○ 4-digit or ○ No social security number, pursuant to Chapter 119, Florida Statutes, or other applicable laws.

## II. Definitions

For the purposes of this MOU, the below-listed terms shall have the following meanings:

**A. Batch/File Transfer Protocol (FTP)/Secure File Transfer Protocol (SFTP)** - An electronic transfer of data in a secure environment.

**B. Business Point-of-Contact -** A person appointed by the Requesting Party to assist the Providing Agency with the administration of the MOU.

**C. Consumer Complaint Point-of-Contact** - A person appointed by the Requesting Party to assist the Providing Agency with complaints from consumers regarding misuse of personal information protected under DPPA.

**D. Control Record** - A record containing fictitious information that is included in data made available by the Providing Agency and is used to identify inappropriate disclosure or misuse of data.

**E. Crash Insurance Inquiry** - Insurance information, such as insurance company name, policy type, policy status, insurance creation and expiration date, including insurance policy number, provided to the Requesting Party pursuant to Section 324.242(2), Florida Statutes. Such inquiry is to be made on only vehicles involved in a crash. The Vehicle Identification Number (VIN) on which such inquiry is made must be involved in the crash for which a crash report number and the date of crash is submitted to the Providing Agency.

**F. Downstream Entity** - Any individual, association, organization, or corporate entity who receives driver license and/or motor vehicle data from a Third Party End User in accordance with DPPA and Section 119.0712(2), Florida Statutes.

**G. Driver License Information** - Driver license and identification card data collected and maintained by the Providing Agency. This data includes personal information as defined in item N, below.

**H. Driver Privacy Protection Act (DPPA)** - The Federal Act (see, 18 United States Code § 2721, et seq.) that prohibits release and use of personal information except as otherwise specifically permitted within the Act.

**I. Government Entity** - Any federal, state, county, county officer, or city government, including any court or law enforcement agency.

**J. Highly Restricted Personal Information** - Includes, but is not limited to, medical or disability information or social security number.

**K. Insurance Record** - Insurance information, such as insurance company name, policy type, policy status, insurance creation and expiration date, but excluding insurance policy number, provided to the Requesting Party, pursuant to Section 324.242(2), Florida Statutes.

**L. Motor Vehicle Information** - Title and registration data collected and maintained by the Providing Agency for vehicles. This information includes personal information as defined in item N, below.

**M. Parties** - The Providing Agency and the Requesting Party.

**N. Personal Information** - As described in Section 119.0712(2)(b), Florida Statutes and 18 U.S.C. S.2725, information found in the motor vehicle or driver record which includes, but is not limited to, the subject's driver identification number, name, address, (but not the 5 – digit zip code) and medical or disability information.

**O. Private Entity** - Any entity that is not a unit of government, including, but not limited to, a corporation, partnership, limited liability company, nonprofit organization or other legal entity or a natural person.

**P. Providing Agency** - The Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to driver license and/or motor vehicle data to the Requesting Party.

**Q. Registration Hold** - A hold placed on the owner, vehicle or registration, intended to prevent extension or renewal of any motor vehicle registration.

**R. Requesting Party** - Any entity type that is expressly authorized by Section 119.0712(2), Florida Statutes and DPPA to receive personal information and/or highly restricted personal information that requests information contained in a driver license or motor vehicle record from the Providing Agency through remote electronic access.

**S. Requesting Party Number** - A unique number assigned to the Requesting Party by the Providing Agency that identifies the type of record authorized for release and the associated statutory fees. Misuse of a Requesting Party Number to obtain information is strictly prohibited and shall be grounds for termination in accordance with Section X, Termination and Suspension.

**T. Technical Contact** - A person appointed by the Requesting Party to oversee the maintenance/operation of setting up of Web Service and Batch/FTP/SFTP processes.

**U. Third Party End User** - Any individual, association, organization, or corporate entity who receives driver license and/or motor vehicle data from the Requesting Party in accordance with DPPA and Section 119.0712(2), Florida Statutes.

**V. Web Service** - A service where the Requesting Party writes a call program to communicate with the Web Service of the Providing Agency to receive authorized motor vehicle and driver license data.

## III. Legal Authority

The Providing Agency maintains computer databases containing information pertaining to driver's licenses and motor vehicles pursuant to Chapters 317, 319, 320, 322, 328, and Section 324.242(2), Florida Statutes. The driver license, motor vehicle, and vessel data contained in the Providing Agency's databases is defined as public record pursuant to Chapter 119, Florida Statutes; and as such, is subject to public disclosure unless otherwise exempted by law.

As the custodian of the state's driver and vehicle records, the Providing Agency is required to provide access to records permitted to be disclosed by law.

Under this MOU, the Requesting Party will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party agrees to maintain the confidential and exempt status of any and all information provided by the Providing Agency pursuant to this MOU and to ensure that any Third Party End Users accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law. In addition, the Requesting Party agrees that insurance policy information shall only be utilized pursuant to Section 324.242(2), Florida Statutes.

This MOU is governed by the laws of the State of Florida and jurisdiction of any dispute arising from this MOU shall be in Leon County, Florida.

## IV. Statement of Work

**A.** The Providing Agency agrees to:

1. Provide the Requesting Party with the technical specifications, and Requesting Party Number if applicable, required to access data in accordance with the access method being requested.

2. Allow the Requesting Party to electronically access data as authorized under this MOU.

3. Collect all fees for providing the electronically requested data, pursuant to applicable Florida Statutes, rules and policies, including Sections 320.05 and 322.20, Florida Statutes. The fee shall include all direct and indirect costs of providing remote electronic access, according to Section 119.07(2)(c), Florida Statutes.

4. Collect all fees due for electronic requests through the Automated Clearing House account of the banking institution which has been designated by the Treasurer of the State of Florida for such purposes.

5. Terminate the access of the Requesting Party for non-payment of required fees. The Providing Agency shall not be responsible for the failure, refusal, or inability of the Requesting Party to make the required payments, or interest on late payments for periods of delay attributable to the action or inaction of the Requesting Party.

6. Notify the Requesting Party thirty (30) business days prior to changing any fee schedules, when it is reasonable and necessary to do so, as determined by the Providing Agency. All fees are established by Florida law. Any changes in fees shall be effective on the effective date of the corresponding law change. The Requesting Party may continue with this MOU as modified or it may terminate the MOU in accordance with Section X., subject to the payment of all fees incurred prior to termination.

7. Perform all obligations to provide access under this MOU contingent upon an annual appropriation by the Legislature.

8. Provide electronic access to driver license and/or motor vehicle information pursuant to roles and times established other than scheduled maintenance or periods of uncontrollable disruptions. Scheduled maintenance normally occurs Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M.

9. Provide a contact person for assistance with the implementation of this MOU.

**B.** The Requesting Party agrees to:

1. Use information only for the expressed purposes as described in Attachment I of this MOU.

2. Self-report to the Providing Agency all violations of the MOU within five (5) business days of discovery of such violation(s). The report shall include a description, the time period, the number of records impacted, the harm caused, and all steps taken as of the date of the report to remedy or mitigate any injury caused by the violation.

3. Accept responsibility for interfacing with any and all Third Party End Users. The Providing Agency will not interact directly with any Third Party End Users. Requesting Party shall not give Third Party End Users the name, e-mail address, and/or telephone number of any Providing Agency employee without the express written consent of the Providing Agency.

4. Establish procedures to ensure that its employees and agents comply with Section V, Safeguarding Information and provide a copy of the procedures to the Providing Agency within ten (10) business days of a request.

5. Not assign, sub-contract, or otherwise transfer its rights, duties, or obligations under this MOU without the express written consent and approval of the Providing Agency.

6. Use the information received from the Providing Agency only for the purposes authorized by this MOU. The Requesting Party shall not share or provide any information to another unauthorized entity, agency or person.

7. Protect and maintain the confidentiality and security of the data received from the Providing Agency in accordance with this MOU and applicable state and federal laws.

8. Indemnify the Providing Agency and its employees from any and all damages arising from the Requesting Party's negligent or wrongful use of information provided by the Providing Agency, to the extent allowed by law.

9. For Federal agencies: The Requesting Party agrees to promptly consider and adjudicate any and all claims that may arise out of this MOU resulting from the actions of the Requesting Party, duly authorized representatives, agents, or contractors of the Requesting Party, and to pay for any damage or injury as may be required by federal law. Such adjudication will be pursued under the Federal Tort Claims Act, 28 U.S.C. § 2671 et seq., the Federal Employees Compensation Act, 5 U.S.C. § 8101 et seq., or such other federal legal authority as may be pertinent.

10. Update user access/permissions upon reassignment of users within five (5) business days.

11. Immediately inactivate user access/permissions following separation, or negligent, improper, or unauthorized use or dissemination of any information.

12. For all records containing Personal Information released to a Third Party End User, maintain records identifying each person or entity that receives the personal information and the permitted purpose for which it will be used for a period of five (5) years. The Requesting Party shall provide these records or otherwise make these records available for inspection within five (5) business days of a request by the Providing Agency.

13. Pay all costs associated with electronic access of the Providing Agency's driver license and/or motor vehicle information. The Requesting Party shall:

    a. Maintain an account with a banking institution as required by the Providing Agency.

    b. Complete and sign the appropriate document(s) to allow the Providing Agency's designated banking institution to debit the Requesting Party's designated account.

    c. Pay all fees due the Providing Agency by way of the Automated Clearing House account of the Providing Agency's designated banking institution. Collection of transaction fees from eligible and authorized Third Party End Users is the responsibility of the Requesting Party.

14. Notify the Providing Agency within five (5) business days of any changes to the name, address, telephone number and/or email address of the Requesting Party, its Point-of-Contact for Consumer Complaints, and/or its Technical Contact. The information shall be e-mailed to DataListingUnit@flhsmv.gov. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.

15. Immediately notify the Providing Agency of any change of FTP/SFTP for the receipt of data under this MOU. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.

16. Understand that this MOU is subject to any restrictions, limitations or conditions enacted by the Florida Legislature, which may affect any or all terms of this MOU. The Requesting Party understands that they are obligated to comply with all applicable provisions of law.

17. Timely submit statements required in Section VI. Compliance and Control Measures, subsections B and C.

18. A Requesting Party who has not previously received records from the Providing Agency shall utilize web services currently offered by the Providing Agency rather than batch/FTP/SFTP processes. Also, any Requesting Party using the FTP/SFTP processes agrees to transition to web services, where available, within six months (6) months of the Providing Agency's request.

19. The Requesting Party shall cooperate and ensure that its subcontractors, if any, cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing pursuant to section 20.055, Florida Statutes.

20. If the Requesting Party has a public facing website that allows an individual to obtain driver license and/or motor vehicle information, the following minimum requirements must be in place prior to the transmission of data:

    a. Safeguards to ensure information obtained through the website is only disclosed to individuals authorized to receive it under 18 U.S.C. §2721(b). This includes internal controls to prevent or detect instances in which an individual attempts to purchase a record other than their own and/or to verify that the requestor meets a DPPA exemption.

    b. If the Requesting Party intends to allow an individual to purchase their own transcript from the Requesting Party's website utilizing the DPPA exemption provided by 18 U.S.C. §2721(b)(13),, a process to verify that the payment instrument used to authorize the purchase is in the same name as the transcript being requested.

    c. Safeguards to ensure that information is provided through the website only for the expressed purposes as described in Attachment I of this MOU.

    d. Use of Transport Layer Security version 1.2 or later for encryption of data in transit and in session state.

    e. Safeguards to ensure that the website is periodically scanned by a qualified external vendor for system vulnerabilities and all identified vulnerabilities are promptly remediated.

    f. Safeguards to ensure that all systems that process driver license or motor vehicle information adhere to a formalized patch management process.

## V. Safeguarding Information

The Parties shall access, disseminate, use and maintain all information received under this MOU in a manner that ensures its confidentiality and proper utilization in accordance with Chapter 119, Florida Statutes, and DPPA. Information obtained under this MOU shall only be disclosed to persons to whom disclosure is authorized under Florida law and federal laws. Any disclosure of information shall be in accordance with 18 U.S.C. §2721(c). In the event of a security breach, the Requesting Party agrees to comply with the provisions of Section 501.171, Florida Statutes.

Any person who knowingly violates any of the provisions of this section may be subject to criminal punishment and civil liability, as provided in Sections 119.10 and 775.083, Florida Statutes. In addition, any person who knowingly discloses any information in violation of DPPA may be subject to criminal sanctions, including fines, and civil liability.

In an effort to ensure information is only used in accordance with Chapter 119, Florida Statutes, and DPPA, the Providing Agency may include control records in the data provided in an effort to identify misuse of the data.

The Requesting Party shall notify the Providing Agency of any of the following within five (5) business days:

**A.** Termination of any agreement/contract between the Requesting Party and any other State/State Agency due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy. The Requesting Party shall also notify the Providing Agency if any State/State Agency declines to enter into an agreement/contract with the Requesting Party to provide DPPA protected data.

**B.** Any pending litigation alleging DPPA violations or under any state law relating to the protection of driver privacy.

**C.** Any instance where the Requesting Party is found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy.

**D.** Any instance where the owner, officer, or control person of the Requesting Party owned a majority interest in, or acted as a control person of, an entity that was found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy.

**E.** A breach of security as defined by Section 501.171, Florida Statutes.

The Parties mutually agree to the following:

**A.** Information exchanged will not be used for any purposes not specifically authorized by this MOU and its attachments. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this or any unauthorized information to unauthorized persons.

**B.** The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, except as otherwise provided in Section 768.28, Florida Statutes.

**C.** Information obtained from the Providing Agency will be stored in a location that is physically and logically secure from access by unauthorized persons.

**D.** The Requesting Party shall develop security requirements and standards consistent with Section 282.318, Florida Statutes, Florida Administrative Code Rule 60GG-2 (Formerly 74-2, FAC), and the Providing Agency's security policies; and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency security policies are set forth in Attachment III.

**E.** Access to the information received from the Providing Agency will be protected in such a way that

unauthorized persons cannot view, retrieve, or print the information.

**F.** All personnel with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.

**G.** All personnel with access to the information will be instructed of and acknowledge their understanding of the civil and criminal sanctions specified in state and Federal law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.

**H.** All access to the information must be monitored on an ongoing basis by the Requesting Party. In addition, the Requesting Party must complete an Annual Certification Statement to ensure proper and authorized use and dissemination of information and provide it to the Providing Agency pursuant to Section VI. B, below.

**I.** All data received from the Providing Agency shall be encrypted during transmission to Third Party End Users using Transport Layer Security (TLS) version 1.2 or higher encryption protocols. Alternate encryption protocols are acceptable only upon prior written approval by the Providing Agency.

**J.** By signing the MOU, the representatives of the Providing Agency and Requesting Party, on behalf of the respective Parties, attest and ensure that the confidentiality of the information exchanged will be maintained.

## VI. Compliance and Control Measures

**A. Internal Control and Data Security Audit -** This MOU is contingent upon the Requesting Party having appropriate internal controls in place at all times that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a request from the Providing Agency. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. The audit shall certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. The audit must have an original signature of the CPA and the Requesting Party's agency head, owner, officer, or control person designated by Letter of Delegation to execute contracts/agreements on their behalf. The audit shall be sent via Certified U.S. Mail to the Providing Agency as set forth in Section XI, Notices.

**B. Annual Certification Statement -** The Requesting Party shall submit to the Providing Agency an annual statement indicating that the Requesting Party has evaluated and certifies that it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of this MOU and applicable

laws. The Requesting Party shall submit this statement annually, within fifteen (15) business days after the anniversary of the execution date of this MOU. (NOTE: During any year in which an Internal Control and Data Security Audit is conducted, submission of the Internal Control and Data Security Audit may satisfy the requirement to submit an Annual Certification Statement.) Failure to timely submit the certification statement may result in an immediate termination of this MOU.

In addition, prior to expiration of this MOU, if the Requesting Party intends to enter into a new MOU, a certification statement attesting that appropriate controls remained in place during the final year of the MOU and are currently in place shall be required to be submitted to the Providing Agency prior to issuance of a new MOU.

**C. Misuse of Personal Information –** The Requesting Party must notify the Providing Agency in writing of any incident where it is suspected or confirmed that personal information has been compromised as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within five (5) business days of such discovery. The statement must be provided on the Requesting Party's letterhead and include each of the following: a brief summary of the incident; the outcome of the review; the date of the occurrence(s); the number of records compromised; the name or names of personnel responsible; whether disciplinary action or termination was rendered; and whether or not the persons whose personal information was compromised were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Party to ensure that misuse of data does not continue or recur. This statement shall be mailed to the Providing Agency's Bureau Chief of Records at the address indicated in XI, Notices A., above. (NOTE: If an incident involving breach of personal information did occur and the Requesting Party did not notify the owner(s) of the compromised records, the Requesting Party must indicate why notice was not provided.

In addition, the Requesting Party shall comply with the applicable provisions of Section 501.171, Florida Statutes, regarding data security and security breaches, and shall strictly comply and be solely responsible for adhering to the provisions regarding notice provided therein.

**D. Consumer Complaints –** The Requesting Party shall provide a point-of-contact for consumer complaints. In the event the Providing Agency receives a consumer complaint regarding misuse of DPPA protected information, the Requesting Party shall review and investigate the complaint. The Requesting Party shall provide its findings to the Providing Agency within fifteen (15) business days from the date they were notified by the Providing Agency.

Consumer Complaint Point-of-Contact Information:

Name: Elane Costa

Email: ecosta@fortlauderdale.gov

Phone Number: 954-828-3703

**E. Control Records -** In the event a control record inserted into data received by the Requesting Party is used in a manner that does not comply with DPPA or state law, the Requesting Party shall conduct an investigation of any Third Party End Users who obtained the record from the Requesting Party. As part of this provision, the Requesting Party shall also retain the authority to require Third Party End Users to investigate the Downstream Entities' handling and distribution of data subject to DPPA protection and to provide the results of the investigation to the Requesting Party. The Requesting Party shall provide the results of the investigation(s) and the documents and information collected therein to the Providing Agency within fifteen (15) business days.

## VII. Liquidated Damages

Unless the Requesting Party is a state agency, the Providing Agency reserves the right to impose liquidated damages upon the Requesting Party.

Failure by the Requesting Party to meet the established requirements of this MOU may result in the Providing Agency finding the Requesting Party to be out of compliance, and, all remedies provided in this MOU and under law, shall become available to the Providing Agency.

### A. General Liquidated Damages

In the case of a breach or misuse of data due to non-compliance with DPPA, Sections 119.0712(2) and 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy and motor vehicle information, the Providing Agency may impose upon the Requesting Party liquidated damages of up to $25.00 per record.

In imposing liquidated damages, the Providing Agency will consider various circumstances including, but not limited to:

1. The Requesting Party's history with complying with DPPA, Sections 119.0712(2) and 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy;

2. Whether the Requesting Party self-reported violations of this MOU to the Providing Agency prior to discovery by the Providing Agency;

3. Whether the Requesting Party violated this MOU over an extended period of time;

4. Whether the Requesting Party's violation of this MOU directly or indirectly resulted in injury, and the nature and extent of the injury;
5. The number of records involved or impacted by the violation of this MOU;

6. Whether, at the time of the violation, the Requesting Party had controls and procedures that were implemented and reasonably designed to prevent or detect violations of this MOU; and,

7. Whether the Requesting Party voluntarily made restitution or otherwise remedied or mitigated the harm caused by the violation of this MOU.

In lieu of paying liquidated damages upon assessment, the Requesting Party may elect to temporarily suspend the MOU, contingent upon its submission of a written statement agreeing not to obtain data from the Providing Agency through remote electronic means until such time as the liquidated damages are paid in full. Such statement shall be signed by the Requesting Party's authorized representative and shall be submitted to the Providing Agency within five days of receipt of notice that damages are being assessed.

### B. Corrective Action Plan (CAP)

1. If the Providing Agency determines that the Requesting Party is out of compliance with any of the provisions of this MOU and requires the Requesting Party to submit a CAP, the Providing Agency may require the Requesting Party to submit a Corrective Action Plan (CAP) within a specified timeframe. The CAP shall provide an opportunity for the Requesting Party to resolve deficiencies without the Providing Agency invoking more serious remedies, up to and including MOU termination.

2. In the event the Providing Agency identifies a violation of this MOU, or other non-compliance with this MOU, the Providing Agency shall notify the Requesting Party of the occurrence in writing. The Providing Agency shall provide the Requesting Party with a timeframe for corrections to be made.

3. The Requesting Party shall respond by providing a CAP to the Providing Agency within the timeframe specified by the Providing Agency.

4. The Requesting Party shall implement the CAP only after the Providing Agency's approval.

5. The Providing Agency may require changes or a complete rewrite of the CAP and provide a specific deadline.

6. If the Requesting Party does not meet the standards established in the CAP within the agreed upon timeframe, the Requesting Party shall be in violation of the provisions of this MOU and shall be subject to liquidated damages and other remedies including termination of the MOU.

Except where otherwise specified, liquidated damages of $25.00 per day may be imposed on the Requesting Party for each calendar day that the approved CAP is not implemented to the satisfaction of the Providing Agency.

## VIII. Agreement Term

This MOU shall take effect upon the date of last signature by the Parties and shall remain in effect for three (3) years from this date unless terminated or cancelled in accordance with Section X, Termination and Suspension. Once executed, this MOU supersedes all previous agreements between the parties regarding the same subject matter.

## IX. Amendments

This MOU incorporates all negotiations, interpretations, and understandings between the Parties regarding the same subject matter and serves as the full and final expression of their agreement. This MOU may be amended by written agreement executed by and between both Parties. Any change, alteration, deletion, or addition to the terms set forth in this MOU, including to any of its attachments, must be by written agreement executed by the Parties in the same manner as this MOU was initially executed. If there are any conflicts in the amendments to this MOU, the last -executed amendment shall prevail. All provisions not in conflict with the amendment(s) shall remain in effect and are to be performed as specified in this MOU.

## X. Termination and Suspension

**A.** This MOU may be unilaterally terminated for cause by either party upon finding that the terms and conditions contained herein have been breached by the other party. Written notice of termination shall be provided to the breaching party; however, prior-written notice is not required and notice may be provided upon cessation of work under the agreement by the non-breaching party.

**B.** In addition, this MOU is subject to unilateral suspension or termination by the Providing Agency without notice to the Requesting Party for failure of the Requesting Party to comply with any of the requirements of this MOU, or with any applicable state or federal laws, rules, or regulations, including, but not limited to, DPPA, Sections 119.0712(2) and 501.171, Florida Statutes, or any laws designed to protect driver privacy.

**C.** This MOU may also be cancelled by either party, without penalty, upon thirty (30) business days advanced written notice to the other party. All obligations of either party under the MOU will remain in full force and effect during the thirty (30) business day notice period.

**D.** This MOU may be terminated by the Providing Agency if the Requesting Party, or any of its majority owners, officers or control persons are found by a court of competent jurisdiction to have violated any provision of any state or federal law governing the privacy and disclosure of personal information. This MOU may be terminated in the event any agreement/contract between the Requesting Party and any other state/state agency is terminated due to non-compliance with DPPA or data breaches, or any state laws designed to protect driver privacy. The Requesting Party will have 10 days from any action described above to provide mitigating information to the Providing Agency. If submitted timely, the Providing Agency will take the mitigation into account when determining whether termination of the MOU is warranted.

## XI. Notices

Any notices required to be provided under this MOU shall be sent via Certified U.S. Mail and email to the following individuals:

For the Providing Agency:

Chief, Bureau of Records
2900 Apalachee Parkway
Tallahassee, Florida 32399
Tel: (850) 617-2702
Fax: (850) 617-5168
E-mail: DataListingUnit@flhsmv.gov

For the Requesting Party:

Requesting Party's Business Point-of-Contact listed on the signature page.

## XII. Additional Database Access/Subsequent MOU's

The Parties understand and acknowledge that this MOU entitles the Requesting Party to specific information included within the scope of this MOU. Should the Requesting Party wish to obtain access to other personal information not provided hereunder, the Requesting Party will be required to execute a subsequent MOU with the Providing Agency specific to the additional information requested. All MOU's granting access to personal information will contain the same clauses as are contained herein regarding audits, report submission, and the submission of Certification statements.

The Providing Agency is mindful of the costs that would be incurred if the Requesting Party was required to undergo multiple audits and to submit separate certifications, audits, and reports for each executed MOU. Accordingly, should the Requesting Party execute any subsequent MOU's with the Providing Agency for access to personal information while the instant MOU remains in effect, the Requesting Party may submit a written request, subject to Providing Agency approval, to submit one of each of the following covering all executed MOU's: Certification; Audit; and/or to have conducted one comprehensive audit addressing internal controls for all executed MOU's. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind an approved request based upon the Requesting Party's compliance with this MOU and/or any negative audit findings.

## XIII. Public Records Requirements

The parties to this MOU recognize and acknowledge that any agency having custody of records made or received in connection with the transaction of official business remains responsible for responding to public records requests for those records in accordance with applicable law (specifically, Chapter 119, Florida Statutes) and that public records that are exempt or confidential from public records disclosure requirements will not be disclosed except as authorized by law.

If the Requesting Party is a "contractor" as defined in Section 119.0701(1)(a), Florida Statutes, the Requesting Party agrees to comply with the following requirements of Florida's public records laws:

1. Keep and maintain public records required by the Providing Agency to perform the service.

2. Upon request from the Providing Agency's custodian of public records, provide the Providing Agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law.

3. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the Requesting Party does not transfer the records to the Providing Agency.

4. Upon termination or expiration of the MOU, the Requesting Party agrees they shall cease disclosure or distribution of all data provided by the Providing Agency. In addition, the Requesting Party agrees that all data provided by the Providing Agency remains subject to the provisions contained in DPPA and Sections 119.0712 and 501.171, Florida Statutes.

**IF THE REQUESTING PARTY HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE REQUESTING PARTY'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFiling@flhsmv.gov, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, and STE. A432, TALLAHASSEE, FL 32399-0504.**

**REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK**

**IN WITNESS HEREOF,** the Parties hereto, have executed this MOU by their duly authorized officials on the date(s) indicated below.

**REQUESTING PARTY:**

ATTEST:

_____
Jeffrey A. Modarelli, City Clerk

Address:

_____

City, State & Zip:

_____

CITY OF FORT LAUDERDALE, a municipal corporation of the State of Florida.

By _____
Christopher J. Lagerbloom, ICMA-CM
City Manager

Date: _____

Approved as to form:
Alain E. Boileau, City Attorney

_____
Shari C. Wallen, Esq.
Assistant City Attorney

**BUSINESS POINT-OF-CONTACT:**

_____
Printed/Typed Name

_____
Official Requesting Party Email Address

_____
Phone Number / Fax Number

**TECHNICAL POINT-OF-CONTACT:**

_____
Printed/Typed Name

_____
Official Requesting Party Email Address

_____
Phone Number / Fax Number

**PROVIDING AGENCY:**

Florida Department of Highway Safety and Motor Vehicles
Providing Agency Name

2900 Apalachee Parkway
Street Address

_____
Suite

Tallahassee, Florida 32399
City State Zip Code

**BY:**

_____
Signature of Authorized Official

_____
Printed/Typed Name

_____
Chief, Bureau of Purchasing and Contracts

_____
Date

_____
Official Providing Agency Email Address

_____
Phone Number

# ATTACHMENT I

## FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES Request For Exempt Personal Information In A Motor Vehicle/Driver License Record

The Driver's Privacy Protection Act, 18 United States Code sections 2721("DPPA") makes personal information contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle or driver license record includes, but is not limited to, an individual's social security number, driver license or identification number, name, address and, medical or disability information. Personal information does not include information related to driving violations and driver status. Personal information from these records may only be released to individuals or organizations that qualify under one of the exemptions provided in DPPA, which are listed on the back of this form.

In lieu of completing this form, a request for information may be made in letter form (on company/agency letterhead, if appropriate) stating the type of information being requested, the DPPA exemption(s) under which the request is being made, a detailed description of the how the information will be used, and a statement that the information will not be used or redisclosed except as provided in DPPA. If the information is provided on letterhead it must include a statement that the information provided is true and correct, signed by the authorized official under penalty of perjury, and notarized.

I am a representative of an organization requesting personal information for one or more records as described below. I declare that my organization is qualified to obtain personal information under exemption number(s) 1_____, as listed on page 3 of this form.

I understand that I shall not use or redisclose this personal information except as provided in DPPA and that any use or redisclosure in violation of these statutes may subject me to criminal sanctions and civil liability.

Complete the following for each DPPA exemption being claimed. (attached additional page, if necessary):

| DPPA Exemption Claimed: | Description of How Requesting Party Qualifies for Exemption: | Description of how Data will be used: |
|---|---|---|
| 1 | Government Agency | To issue parking citations |
| | | |

Obtaining personal information under false pretenses is a state and federal crime. Under penalties of perjury, I declare that I have read the foregoing Request For Exempt Personal Information in A Motor Vehicle/Driver License Record and that the facts stated in it are true and correct.

**AGENCY**

ATTEST:

CITY OF FORT LAUDERDALE, a municipal corporation of the State of Florida.

_____
Jeffrey A. Modarelli, City Clerk

By _____
Christopher J. Lagerbloom, ICMA-CM
City Manager

Approved as to form:
Alain E. Boileau, City Attorney

_____
Shari C. Wallen, Esq.
Assistant City Attorney

STATE OF FLORIDA
COUNTY OF BROWARD

The foregoing instrument was acknowledged before me by means of □ physical presence or □ online notarization, this ____ day of _____, 20__, by Christopher J. Lagerbloom, ICMA-CM as City Manager of the City of Fort Lauderdale, Florida, a municipal corporation.

(SEAL)

_____
Signature of Notary Public – State of Florida

_____
Print, Type, or Stamp Commissioned Name of Notary Public

Personally Known ____ OR Produced Identification ____
Type of Identification Produced _____

Pursuant to section 119.0712(2), F. S., personal information in motor vehicle and driver license records can be released for the following purposes, as outlined in 18 United States Code, section 2721.

Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321-331 of title 49, and, subject to subsection (a)(2), may be disclosed as follows.

1. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

2. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

3. For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only -
(a) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
(b) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

4. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

5. For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

6. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

7. For use in providing notice to the owners of towed or impounded vehicles.

8. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.

9. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.

10. For use in connection with the operation of private toll transportation facilities.

11. For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.

12. For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.

13. For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.

14. For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.

**Agency/Business Name:** City of Fort Lauderdale

## DATA ACCESS SPECIFICATIONS

### ATTACHMENT II - Jobs and Processes Selected

| Mode of Access | | Type of Data requested | | Statutory Fees (subject to change by the Legislature) | | |
|---|---|---|---|---|---|---|
| Batch (FTP) | | DL Data | | $0.01/record, per Sec 322.20, F. S. | | No Charge |
| | | MV Data | | $0.01/record, per Sec 320.05, F.S. | | No Charge |
| | | DL Status (DSS600/605) | | $0.01, $0.50, $2.00/record, per Sec 320.05, F.S. | | No Charge |
| Program/Job Name | | | | | | |
| IP Address(es) | | | | | | |
| **Web Services** | | | | | | |
| Driver Transcript Web Service | | DL Transcript (3 Year) (old DTR060) | | $8.00; $2.00/record not found/Sec. 322.20, F.S. | | No Charge |
| | | DL Transcript (7 Year or Complete) (old DTR060) | | $10.00; $2.00/record not found/Sec. 322.20, F.S. | | No Charge |
| | | Bulk Lookback (old DMS485) | | $0.01/record; $2.00/record not found/Sec 322.20, F.S. | | No Charge |
| | | | | | | |
| Public Access Web Service | | DL Status | | $0.50/ record, per Sec 320.05, F.S. | | No Charge |
| | | MV Record | | $0.50/ record, per Sec 320.05, F.S. | | No Charge |
| | | Insurance Record | | $0.50/ record, per Sec 320.05, F.S. | | No Charge |
| | | Parking Permit Record | | $0.50/ record, per Sec 320.05, F.S. | | No Charge |
| | | | | | | |
| Penny Vendor DL Web service | | DL update file of issuance/ purge records (old DFO292) | | $0.01/record, per Sec 322.20, F. S. | | No Charge |
| | | | | | | |
| Renewal Notification Web service | | MV renewal file | | | | No charge |
| | | | | | | |
| Residency Verification Web service | | Residency Verification | | | | No charge |
| | | | | | | |
| Other Web Services | | | | | | No charge |

FLHSMV
FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

# Data Access Application

Prior to executing the Memorandum of Understanding (MOU) for Driver License and/or Motor Vehicle Data Exchange, the Requesting Party is required to complete this application. Please use additional pages as necessary.

1. In the last ten (10) years, has any agreement/contract between the Requesting Party and/or any other State/State Agency been terminated due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy? Yes ○ No ◉ If yes, please explain and supply certified copies of the pertinent documents:

2. In the last ten (10) years, has any State/State Agency declined to enter into an agreement/contract with the Requesting Party to provide DPPA protected data? Yes ○ No ◉ If yes, please explain:

3. Is there any pending litigation against the Requesting Party alleging violations of DPPA or any state law relating to the protection of driver privacy? Yes ○ No ◉ If yes, please explain and provide a certified copy of the pertinent court documents:

4. In the last ten (10) years, has there been any instance where the Requesting Party has been found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy? Yes ○ No ◉ If yes, please explain and provide certified copies of the pertinent documents:

5. In the last ten (10) years, has there been any instance where an owner, officer, or control person[1] of the Requesting Party who owned a majority interest in, or acted as a control person of, an entity that was found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy? Yes ○ No ⊙ If yes, please explain and provide certified copies of the pertinent documents:

6. In the last ten (10) years, has there been any breach of security as defined by Section 501.171, Florida Statutes? Yes ○ No ⊙ If yes, provide details of each breach and discuss all safeguards implemented as a result of the breach of security:

7. How you will ensure that all personnel with access to the information exchanged under the terms of the MOU are instructed of, and acknowledge their understanding of, the confidential nature of the information?

8. Does your company or agency have a public facing website that allows an individual to purchase driver license/motor vehicle information? Yes ○ No ⊙

   If yes, please provide the URL: _____

   In addition, please indicate whether your agency has the following minimum requirements listed below in place:

   A. Safeguards to ensure information obtained through the website is only disclosed to individuals authorized to receive it under 18 U.S.C. §2721(c). This includes internal controls to prevent or detect instances in which an impostor attempts to purchase a record other than their own and/or to verify that the requestor meets a DPPA exemption. ○ Yes ○ No ⊙ N/A

      Please describe safeguards:



[1] Control Person, for these purposes, means the power, directly or indirectly, to direct the management or policies of a company, whether through the ownership of securities, by contract, or otherwise. Any person that (i) is a director, general partner, or officer exercising executive responsibility (or having similar status or functions); (ii) directly or indirectly has the right to vote 25% or more of a class of a voting security or has the power to sell or direct the sale of 25% or more of a class of voting securities; or (iii) in the case of a partnership, has the right to receive upon dissolution, or has contributed, 25% or more of the capital, is presumed to control that company.

B. Do you intend to allow individuals to purchase their own transcript from your public facing website, utilizing DPPA exemption number 13? Yes○ No○ N/A◉

C. If the answer to the previous question is yes, do you have a process in place to verify that the payment instrument used to authorize the purchase is in the same name as the transcript being requested? Yes○ No○ N/A◉

Please explain the process:

D. Do you only provide information through the website for the expressed purposes as described in Attachment I of this MOU? Yes○ No○ N/A◉

E. Does the website utilize Transport Layer Security version 1.2 or later for encryption of data in transit and in session state? Yes○ No○ N/A◉

Please explain:

F. Is the website periodically scanned by a qualified external vendor for system vulnerabilities? Yes○ No○ N/A◉

G. If the answer to the previous question is yes, are identified vulnerabilities promptly remediated? Yes○ No○ N/A◉

Please explain:

9. Do all systems that process driver license / motor vehicle information adhere to a formalized patch management process? Yes◉ No○

Please explain:

Patches are up to date and on time.

In addition, the following documents are required:

a. A copy of your business license.
b. A copy of your State of Florida corporation licensure or certification.
c. If providing services on behalf of a government entity, provide the supporting documentation to show or prove you are entitled to the DPPA exemption claimed. For example, a letter from each entity confirming the type of service being provided and/or an agreement with an entity authorizing you to conduct services.

Under penalty of perjury, I affirm that the information provided in this document is true and correct.

**AGENCY**

ATTEST:

CITY OF FORT LAUDERDALE, a municipal corporation of the State of Florida.

_____
Jeffrey A. Modarelli, City Clerk

By _____
Christopher J. Lagerbloom, ICMA-CM
City Manager

Approved as to form:
Alain E. Boileau, City Attorney

_____
Shari C. Wallen, Esq.
Assistant City Attorney

STATE OF FLORIDA
COUNTY OF BROWARD

The foregoing instrument was acknowledged before me by means of □ physical presence or □ online notarization, this ____ day of _____, 20__, by Christopher J. Lagerbloom, ICMA-CM as City Manager of the City of Fort Lauderdale, Florida, a municipal corporation.

(SEAL)

_____
Signature of Notary Public – State of Florida

_____
Print, Type, or Stamp Commissioned Name of Notary Public

Personally Known ____ OR Produced Identification ____
Type of Identification Produced _____

**Terry L. Rhodes**
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

**Data Access Technical Specifications Questionnaire**

**Agency:** City of Fort Lauderdale

I. **Access Method or Condition.** The Requesting Party shall attest to their respective statutory eligibility by completing the Florida Department of Highway Safety and Motor Vehicles Request for Exempt Personal information in a Driver License/Motor Vehicle Record form.

II. **Access Specifications.** Please provide a description of the specific data being requested, the statutory authority/DPPA exemption, and which method of receiving the data is being requested in the space below:

| Description of specific data needed | Description of specific use of data, to **include statutory and/or DPPA authority to receive data.** |
|---|---|
| | |

III. **Method of receiving/accessing data:**

**Public Access / Web service**: This service provides basic driver information and eligibility. It also provides motor vehicle information. This service is available to private agencies for $0.50 per record search and is at no charge for governmental agencies.

**Driver Transcript / Web Service**: 3 year, 7 year and complete driver license transcripts are available through this service. This service is available to private, city and county agencies for $8.00 for a 3 year transcript and $10.00 for a 7 year or complete transcript per record. Transcripts are provided at no charge to law enforcement agency, federal and state agencies.

The requestor's software communicates with our software over the Internet; The API specification for the driver transcripts and public access web service can be found within the following URL: https://betaservices.flhsmv.gov/transcripts/ and URL: https://betaservices.flhsmv.gov/PublicAccess/. Access is by a user id and a password. There is no web page, as such, for the user.

**Batch/FTP**: The requestor submits a file with multiple records that they want matched through a standard file transfer protocol (SFTP) from their server to one of ours. Our processes pulls the file, run a program or series of programs, and return matching records or records meeting established criteria by FTP for the requestor to pick up. Driver license transcripts, DL status check, motor vehicle records, can be provided in this process also. Note: the requesting party must transition to web services as they become available for these processes.

We have different kinds of FTP processes to suit your various needs. A few are listed below.

DMS485 - This program provides a driver transcript. This program reviews each record and returns transcripts for only those driver records who have had a sanction or a conviction added onto their record within the past 1, 3, 6,12 24 or 36 month (lookback) period. A transcript will NOT be returned on those drivers who do not meet the above criteria. Transcripts requested can be ($8.00) 3 year, ($10.00) 7 year or ($10.00) complete; $2.00 for record not found and $0.01 for a DL# not meeting the criteria.

DSS600/605 - This does not provide a driver transcript but will provide pertinent information only on those drivers whose status is ineligible. You will receive such information as the type of sanction, reason, and effective date. A response will not be given on eligible drivers. License type is NOT provided in the output file. A fee of .50 for each inquiry whose status is ineligible and a fee of .01 for all drivers whose status is eligible. This service is free to all government agencies.

DTR060 - Driver license transcript programs/ Returns transcripts on all DL# provided, no criteria set. This service is available to private entities, city, county and governmental agencies for $8.00 for a 3 year transcript and $10.00 for a 7 year or complete transcript per record. Transcripts are at no charge to LEA, federal and state agencies.

DL/MV database - We also provide a Driver License and Motor Vehicle Database for $0.01 per record, with weekly or monthly updates.

**Payment process**: Automatic debits to your bank account will be made whenever the services are utilized. Prior to setup for above services, a debit authorization form should be completed by you and your banking institution and returned to us. This will allow DHSMV to debit your account. Please note that there is no other method of payment when utilizing the above services for a charge.

**AGENCY**

ATTEST:

CITY OF FORT LAUDERDALE, a municipal corporation of the State of Florida.

_____
Jeffrey A. Modarelli, City Clerk

By _____
Christopher J. Lagerbloom, ICMA-CM
City Manager

Date: _____

Approved as to form:
Alain E. Boileau, City Attorney

_____
Shari C. Wallen, Esq.
Assistant City Attorney

**Web Application Access**

**Contact Information of the person and serves as liaison for DHSMV**

_____

**Printed/typed Name**

_____

**E-Mail Address**

_____

**Phone Number**

_____

If you are not a governmental agency, please include the company's articles of incorporation or certificate with the Florida Division of Corporations along with FEIN number

FLHSMV
FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

# CERTIFICATION STATEMENT

Under penalty of perjury I have read the requirements contained in the Memorandum of Understanding, Florida Administrative Code, Rule Chapter 60GG-2 (Formerly 74-2, FAC), and the Department of Highway Safety and Motor Vehicles External Information Security Policy and declare that the following is true:

The Requesting Party, The City of Fort Lauderdale, Florida hereby certifies that the Requesting Party has appropriate internal controls in place to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. This includes policies/procedures in place for both personnel to follow and data security procedures/policies to protect personal data. The data security procedures/policies have been approved by a Risk Management IT Security Professional.

ATTEST:

_____
Jeffrey A. Modarelli, City Clerk

CITY OF FORT LAUDERDALE, a municipal corporation of the State of Florida.

By _____
Christopher J. Lagerbloom, ICMA-CM
City Manager

Approved as to form:
Alain E. Boileau, City Attorney

_____
Shari C. Wallen, Esq.
Assistant City Attorney

STATE OF FLORIDA
COUNTY OF BROWARD

The foregoing instrument was acknowledged before me by means of □ physical presence or □ online notarization, this ____ day of _____, 20__, by Christopher J. Lagerbloom, ICMA-CM as City Manager of the City of Fort Lauderdale, Florida, a municipal corporation.

(SEAL)

_____
Signature of Notary Public – State of Florida

_____
Print, Type, or Stamp Commissioned Name of Notary Public

Personally Known ____ OR Produced Identification ____
Type of Identification Produced _____

**This page is intentionally blank**

**The remainder of this file is for reference and/or future use.**

FLHSMV

FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES

ATTACHMENT III

# Department of Highway Safety and Motor Vehicles

## Prepared By:
## Office of Enterprise Security Management

## External Information Security Policy

# Revision History

| Version | Author | Release Notes | Issue Date |
|---|---|---|---|
| 1.2* | Joe Cipriani | Baseline document | 9/30/2015 |
| 1.21 | Tom Trunda | Add definitions and clarifications | 03/17/2016 |
| 2.0 | Scott Morgan and Carl Ford (HSMV) in conjunction with the Tax Collector InfoSec Coalition - Terry Skinner, Kirk Sexton, Dan Andrews and the Honorable Ken Burton Jr., Tax Collector, Manatee County | Revised to align with Department policies in congruence with requirements for External Entities. Added scope for further clarification and applicability. Revised to align with Rule 74-2, F.A.C., Information Technology Security | 08/18/2017 |
| 2.0 | Scott Morgan | Removed draft watermark, formatting check; added statutory reference for F.S., 282.318 in the footer, added effective issue date | 12/7/2017 |

* Note: The document version coincides with the IT Security Policy Manual.

# External Information Security Policy

**Scope**:

This policy applies to all agents, vendors, contractors and consultants (External Entities) who use and/or have access to Department information resources. External Entities who use and/or have access to Department information resources shall adhere to the policies outlined herein. The authority for these policies derives from Florida Statutes 282.318, Security of Data and Information Technology Resources and Florida Administrative Code Chapter 74-2, Information Technology Security.

| #A-02: Data Security | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #A-02: Data Security

### 1.0 Purpose
To ensure that data is protected in all forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This includes any system or process which accesses the State of Florida telecommunications network, or Department information resources, and trusted partners including, but not limited to AAMVA, FDLE and CJIS networks and data.

### 2.0 Policy
Other than data defined as public**,** which may be accessible to public access inquiries (as well as authenticated users), all data and system resources are only accessible on a need-to-know basis to specifically identified, authenticated, and authorized entities.

### 3.0 Data Usage
All users who access Department data must do so only in conformance with this policy. Only uniquely identified, authenticated, and authorized users are allowed access to the Department data, excluding public access inquiries. Access control mechanisms must be utilized to ensure that users can access only that data to which they have been granted explicit access rights.

Information resources are strategic assets vital to the business performance of the Department. These strategic assets must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Department's ability to conduct its mission. Ownership and management of these information resources reside with the Department, and not to any individual or group of individuals.

### 4.0 Data Storage or Transmission
All users who are responsible for the secure storage or transmission of the Department's data must do so only in conformance with this policy. Where confidentiality, privacy or sensitivity requires, stored or transmitted data must be secured via Department-approved encryption technology. This does not supersede provisions of the Public Records Act that states, "computer records are public records," but serves to protect data while stored.

### 5.0 Data Disposal
Access control mechanisms must be utilized to ensure that, during the disposal process, users can access only data to which they have been granted explicit access rights. External Entities shall follow an established process approved by the Department for the disposal of data to include the disposal of confidential data in accordance with The Florida Public Records Act and Federal Standards.

### 6.0 Management Responsibilities
Network operations and systems administration personnel shall ensure that adequate logs and audit trails are maintained. Logs and audit trails must at a minimum record access to data, records, and activation of industry recognized security mechanism for protection of confidential and sensitive data.

## 7.0 Data Classification

The Department is responsible for classification of data. External Entities are required to abide by data classification requirements as outlined by the Department. Data classification shall be done in accordance with Federal Information Processing Standards (FIPS) Publication 199 and is necessary to enable the allocation of resources for the protection of data assets, as well as determining the potential loss or damage from the corruption, loss, or disclosure of data. To ensure the security and integrity of all data, any data asset is Public, Sensitive or Confidential and should be labeled accordingly.

All data falls into one of the following categories:

- Public:
  Information or data that is not classified as sensitive or confidential. Information that, if disclosed outside the State or agency, would not harm the State or Department, its employees, customers, or business partners. This data may be made generally available without specific data custodian approval.

- Sensitive**:**
  Information not approved for general circulation outside the State or Department where its loss would inconvenience the State/Department or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings, and internal project reports. Security at this level is controlled but normal.

- Confidential**:**
  - Data that, by its nature, is exempt from disclosure under the requirements of Chapter 119, F.S.
  - Data whose loss, corruption, or unauthorized disclosure would be a violation of federal or State laws/regulations. Information of a proprietary nature. Procedures, operational work routines, project plans, designs, or specifications that define the way in which the organization operates.
  - Data whose loss, corruption, or unauthorized disclosure would tend to impair business functions or result in any business, financial, or legal loss.
  - Data that involves issues of personal credibility, reputation, or other issues of privacy.
  - Highly sensitive internal documents that could seriously damage the State or Department if such information were lost or made public. Information usually has very restricted distribution and must be protected at all times.

## 8.0 Web Services and Data Exchanges

The Department has created online web-based services and data exchanges which may be utilized by Tax Collectors and authorized Vendors who meet various technical standards, requirements, and statutory authority. The specific standards, requirements, and conditions for use of the aforementioned web services and data exchanges are outlined in the individual Memorandum of Understanding (MOU) for each service offered. The terms and conditions of the MOU shall govern the applicable use, timeframe, and requirements of each web service and data exchange.

| #A-04: Passwords | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #A-04: Passwords

### 1.0 Purpose

To ensure the processes for password creation, distribution, changing, safeguarding, termination, and recovery adequately protect information resources.

### 2.0 Policy and Standards

Passwords are unique strings of characters that personnel or information resources provide in conjunction with a logon ID to gain access to an information resource. Passwords, which are the first line of defense for the protection of the Departments information resources, shall be treated as confidential information and must not be divulged.

1. All user accounts used to access the Department information resources shall have passwords of sufficient strength and complexity, and be implemented based on system requirements and constraints, and in accordance with the following rules to ensure strong passwords are established:
   - Shall be routinely changed at an interval not greater than 90 days.
   - Shall be different than the last 10 passwords.
   - Shall adhere to a minimum length of 8 characters.
   - Shall be a combination of alpha (upper and lower case), numeric, and special characters (unless a particular system does not allow, passwords shall consist of at least 3 of the above 4 categories).
   - Should not be anything that can be easily guessed or associated to the account owner such as: user name, social security number, nickname, relative's names, pet's names, birth date, sports team, etc.
   - Should not be dictionary words or acronyms.
   - Newly created or reset passwords must be randomly generated. Use of a default or standard new/reset password is prohibited.
2. Stored passwords shall be encrypted.
3. Passwords shall not be divulged to anyone. Passwords must be treated as confidential information and shall be safeguarded.
4. Passwords and user names shall not be shared with anyone to include co-workers or contractors. Passwords must be treated as confidential information. Credentials (UserID and passwords) are for exclusive use only by the user to which they are assigned.
5. All users are responsible for the work performed under their credentials (User Id and password). Allowing other users to use your computer while you are logged on is strictly prohibited. Approved exceptions are:
   - Initial System Configuration
   - System Support
   - Troubleshooting Activities

6. If the security of a password is in doubt, the password must be changed immediately.
7. Administrators shall not circumvent this policy solely for ease of use.
8. Users shall not circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Department's ISM. For an exception to be approved, there must be a procedure to change the password.
9. Computing devices shall not be left unattended without enabling a password-protected screensaver that is activated after 15 minutes of inactivity, or logging off the device.
10. User accounts must be locked after 5 unsuccessful login attempts.
11. Passwords must not be transmitted via e-mail or other forms of electronic communication.
12. Passwords must be encrypted during transmission and storage using appropriate encryption technology.
13. Passwords should not be written down and stored at your workstation in your office.
14. Passwords stored on physical media must be protected by an encryption technology outlined in Policy #B-01 Acceptable Encryption.
15. Initial use passwords that have been assigned must expire at the time of first use in a manner that requires the password owner to supply a new password, provided that this functionality is available within that particular product or facility.
16. For all password resets, the identity of the person requesting the password reset must be verified.

| #B-01: Acceptable Encryption | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #B-01: Acceptable Encryption

### 1.0 Overview
To establish policy that directs the use of encryption to provide adequate protection of data where required. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is obtained for the dissemination and use of encryption technologies outside of the United States.

### 2.0 Purpose
To ensure the confidentiality, integrity and availability of data is maintained for Department data and information resources.

### 3.0 Scope
In the event encryption is required for the transmittal of confidential information, the encryption methodology shall be coordinated with the Department's ISM for the management of secure escrow and storage of encryption keys.

### 4.0 Policy
Encryption is the primary means for providing confidentiality for information that can be stored or transmitted, either physically or logically. When possible, confidential information should not be transmitted via email. If confidential information must be sent via email, it shall be encrypted. Information resources that stores or transmits sensitive or confidential data must have the capability to encrypt information.

Proven, standard algorithms must be used as the basis for encryption technologies. Encryption key lengths must be at least 128 bits. The Department key length requirements will be reviewed periodically and upgraded as technology, legislation, or business needs requires.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by and approved by the Department's ISM. It should be noted that the U.S. Government restricts the export of encryption technologies. Potential users of the Department information resources in countries outside the United States should make themselves aware of the encryption technology laws of those countries.

| #B-02: Access Control | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #B-02: Access Control

### 1.0 Purpose

To protect the Department's information resources from threats of unauthorized access, disclosure, modifications, or destruction.

### 2.0 Policy

1. Each user accessing a Department information resource shall be assigned a unique personal identifier, commonly referred to as either a user account, Logon ID, user identification, or User ID. Exceptions: public systems where such access is authorized or for situations where risk analysis by the Department demonstrates such use to be applicable and appropriate. (Example: DL check on the DHSMV website)
2. Users shall not under any circumstances use another user's account logon or credentials.
3. User access rights shall be established based on approved written requests. The user identification shall be traceable to the user for the lifetime of the records or reports in which they appear.
4. A user's access shall be promptly disabled and/or removed from systems which access Department information resources, when access is no longer required. Examples include, but are not limited to, termination, transfer, or removal of the duties that require access. Notification of changes in the status of users with established Department credentials is the responsibility of the authorizing External Entity to report such changes to the Department.
5. Each user shall agree in writing to use the access only for the purpose intended.
6. An automatic workstation time-out shall occur no later than 15 minutes after inactivity. A password shall be required to unlock the user account. User accounts shall be locked after 5 unsuccessful attempts.
   Exception: In the interest of officer safety, devices that are part of a law enforcement vehicle or are used to conduct dispatch functions and are within a physically secure location are exempt from this requirement. However, these devices shall be logged off or locked if they are left unattended.
7. External Entities must monitor the access rights of those whom they have authorized.
8. Established controls must ensure that Department information resources are accessed only by users authorized to do so.
9. Access to accounts with elevated access rights shall follow the principle of least-privilege, and should be restricted to systems personnel only; usage of these accounts shall be logged and subject to audit.
10. Administrative access shall incorporate Separation of Duties to ensure no individual has the ability to control an entire process.
11. Access rights to Department information resources by systems personnel shall be based on specific job requirements. Responsibility for production processing must be separated from

system development, testing and maintenance. Systems or development personnel should only access production data to resolve emergencies.

12. All development and testing shall be performed on test data and not utilize the Department's production data. Test systems shall be kept physically or logically separate from production systems. However, in some instances there is a need to access the Department's production data in a test environment, which requires an exception from the Department's CIO and ISM. The production environment shall not be adversely affected and data shall not be altered. Security controls that provide restricted access and auditing shall not be disabled or removed. Confidential or exempt data shall not be used in any test system.
13. The Department utilizes the principle of least privilege for access control to information resources. All External Entities shall be limited to the access required to do their assigned tasks.
14. Support personnel utilizing remote access to Department information resources for the purpose of providing technical support shall use RDP (Remote Desktop Protocol) or Windows Remote Assistance, or a remote access product approved by the Department's ISM. The following requirements must be met:
    - Remote connectivity must be done in a secure fashion.
    - Remote access must be granted by the end-user or system administrator before a remote session can be initiated.
    - Remote session must be monitored at all times for the duration of the session.
    - Remote session must be terminated immediately upon completion of authorized tasks.

## #B-03: Account Management for User Accounts

### 1.0 Purpose

To ensure that user accounts which access Department information resources are created, maintained, monitored, and removed in a manner that protects Department information resources and user access privileges.

### 2.0 Background

Computer user accounts are the means used to grant access to the Department's information resources. These accounts provide accountability, a key to the Department's computer security program for information resource usage. Creating, controlling, and monitoring all computer user accounts is extremely important for the Department's information resources.

### 3.0 Policy

1. All accounts created must have an associated request and approval that is appropriate for the Department's information resource or service.
2. External Entities must complete Information Security Training on the Department's PartnerNet Portal within 30 days of receiving their account or risk having access terminated.
3. All accounts must be uniquely identifiable using the assigned user name. User accounts and the associated passwords constitute a user's credentials and shall never be shared.
4. All default passwords for accounts must comply with password policy # A-04.
5. All accounts must have a password expiration that complies with password policy # A-04.
6. The appropriate system administrator or other designated staff should disable accounts of individuals on extended leave. Extended leave is defined as greater than 60 days.
7. External Entity user accounts established by the Department that have not been accessed within 30 days are subject to being disabled.
    a. External Entities' System Administrators are responsible for modifying the accounts of individuals that change duties or are separated from their relationship with the External Entity upon notification of change or separation.
    b. Must have a documented process to modify a user account to accommodate situations such as name changes, account changes, and permission changes.
    c. Must have a documented process for periodically reviewing existing accounts for validity.
    d. Department information resources utilized by External Entities are subject to independent audit review of user account management.
    e. Must provide a list of accounts for the systems they administer when requested by authorized Department management.
    f. Must cooperate with authorized Department management investigating security incidents.

## #B-06: Application Service Provider

### 1.0 Purpose

To define minimum security requirements for an Application Service Provider (ASP) to the Department. This policy applies to ASPs that are either being considered for use by the Department or its agent, or have already been selected for use.

### 2.0 Policy and Standards

1. General Security:

    a. The Department reserves the right to audit the infrastructure utilized by the ASP to ensure compliance with this policy. Non-intrusive network audits (basic port scans, etc.) may be performed.
    b. The ASP must provide a proposed architecture document that includes a full network diagram of the Department Application Environment (initially provided to ASP by the Department), illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Department data resides, the applications that manipulate it, and the security thereof.
    c. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.
    d. Exceptions to this policy require prior approval by the Department's ISM and CIO who will evaluate requests on a case-by-case basis.
    e. The ASP must certify compliance to these requirements in writing annually.
    f. The ASP must identify their ISM and provide the Department and authorizing External Entity with contact information.

Physical Security:

a. The ASP's application infrastructure (hosts, network equipment, etc.) must be located in a physically secure facility and in a locked environment.

b. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for the authorizing External Entity.

c. The Department requires that the ASP disclose their ASP background check procedures and results prior to the Department's ISM approval.

3. Network Security:

    a. The network hosting the application must be logically or physically separated from any other network or customer that the ASP may have. This means the authorizing External Entity's application environment must use logically or physically separated hosts and infrastructure.

    b. Data flow between the authorizing External Entity and the ASP:

        - If the Department or the authorizing External Entity will be connecting to the ASP via a private circuit, then that circuit must terminate on the authorizing External Entity's infrastructure, and the operation of that circuit will adhere to this policy.

- If the data between the authorizing External Entity and the ASP traverses a public network such as the Internet, the ASP must deploy appropriate firewall technology, and the traffic between the authorizing External Entity and the ASP must be protected and authenticated by cryptographic technology.

4. Host Security:
   a. The ASP must disclose how and to what extent the hosts or servers (Unix, Windows, etc.) comprising its application infrastructure have been hardened against potential threats and attack vectors. The ASP shall provide any hardening documentation it has for the Department or authorizing External Entity's application infrastructure as well.
   b. The ASP must provide a methodology and plan for ensuring systems are patched or updated according to industry best practices and guidelines. Patches include, but are not limited to, host OS, web server, database, and any other system or application.
   c. The ASP must disclose its processes for monitoring the confidentiality, integrity and availability of those hosts.
   d. The ASP must provide to the Department information on its password policy for the application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
   e. The ASP must provide information on account creation, maintenance, and termination processes, for service, system, and user accounts. This should include information as to how an account is created, how account information is communicated to the user, and how accounts are terminated when no longer needed.
5. Web Security:
   a. The ASP will disclose the use of various web architecture and programming languages, including, but not limited to Java, JavaScript, ActiveX, PHP, Python, C, Perl, VBScript, etc.
   b. The ASP will describe the process for performing security quality assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, or any other activity designed to validate the security architecture.
   c. The ASP will disclose the methodology utilized for web code reviews, including CGI, Java, etc., for the explicit purposes of finding and remediating security vulnerabilities, the authorizing party who performed the review, results of the review, and what remediation activity has taken place.
6. Encryption:
   a. The Department's application data in the custody of the authorizing External Entity must be stored and transmitted using acceptable encryption technology as outlined in Policy #B-01, Acceptable Encryption.
   b. Connections to the ASP utilizing the Internet must be protected using any of the following encryption technologies: IPsec, TLS, SSH/SCP, PGP, or any other encryption technologies approved by the Department's ISM.

| #B-10: Incident Handling (Security Incidents) | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #B-10: Incident Handling (Security Incidents)

### 1.0 Purpose

To ensure that computer security incidents which impacts, or has the potential to impact the confidentiality, integrity, and availability of the Department's information resources are properly recorded, communicated and remediated. Security incidents include, but are not limited to: virus and malware detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources.

### 2.0 Policy

Information security incidents are events involving the Department's information resources, systems, or data, whether suspected or proven, deliberate or inadvertent, that threatens the confidentiality, integrity, and availability, of the Department's information resources. The reporting of incidents enables the Department to review the security controls and procedures; establish additional, appropriate corrective measures, if required, and reduce the likelihood of recurrence.

1. The Department's ISM is responsible for the coordination of any security incident that occurs.

2. Whenever a security incident, such as a virus, Denial of Service, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed that impacts or has the potential to impact the Department's information resources, the Department's ISM must be notified immediately and the appropriate incident management procedures must be followed.

   Reportable Incidents:
   Reportable incidents include, but are not limited to, the following:
   - Physical loss, theft, or destruction of the Department's information resources.
   - Unauthorized disclosure, modification, misuse, or disposal of sensitive, critical, or business-controlled information.
   - Suspected or known unauthorized internal or external access activity, including, but not limited to, sharing of user credentials and accounts must be reported immediately.
   - Unauthorized activity or transmissions using Department information resources.
   - Internal/external intrusions/interference with Department networks (denial of service attacks, unauthorized activity on restricted systems, unauthorized modification or deletion of files, or unauthorized attempts to control information resources.
   - Editing of files when no changes in them should have occurred.
   - Appearance / disappearance of files, or significant /unexpected changes in file size.
   - Systems that display strange messages or that mislabel files and directories.
   - Data that has been altered or destroyed or access that is denied outside of normal business procedures.
   - Detection of unauthorized personnel in controlled information security areas.
   - Lost security tokens, smart cards, identification badges, or other devices used for identification and authentication shall be reported immediately.
   - Fraud, embezzlement, and other illegal activities.
   - Violation of any portion of the External Information Security Policy.

| #B-20: Security Monitoring and Auditing | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #B-20: Security Monitoring and Auditing

### 1.0 Purpose

To ensure that information resource security controls required to protect the Department's information resources are established, effective, and are not being bypassed. This policy defines the requirements and provides the authority for the Department's ISM, and Enterprise Security Management Team (ESM) to conduct audits and risk assessments to ensure integrity of information resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate. This section applies to monitoring inbound and outbound traffic to/from External Entities, agents, and trusted partners' networks and environments. External Entities who access or utilize Department information resources are subject to independent audit review.

### 2.0 Background

Security monitoring allows the Department to detect and mitigate illicit or fraudulent activity as early as possible, therefore limiting the risk of exposure or compromise. Security monitoring can assist in identification and remediation of new security vulnerabilities or emerging threats. This early identification can assist in preventing, or limiting harm to Department information resources.

### 3.0 Policy

1. Security monitoring will be used as a method to confirm that security practices, controls, and policies are functional, adhered to, and are effective.

2. Monitoring consists of activities such as the periodic review of:
   a. Automated intrusion detection system logs
   b. Firewall logs
   c. User account logs
   d. Network scanning logs
   e. Application logs
   f. Data backup recovery logs
   g. Technical Assistance Center (TAC) logs

3. Audits may be conducted to:
   a. Ensure integrity, confidentiality and availability of the Department's information resources
   b. Investigate possible security incidents
   c. Ensure conformance to the Department's security policies
   d. Monitor user or system activity where appropriate

4. The Department shall use automated tools to provide real time notification of detected anomalies or vulnerability exploitation. These tools will be deployed to monitor network traffic and/or operating system security parameters.

5. The following files may be checked for signs of misuse, fraudulent activity, and vulnerability exploitation periodically, or as requested for investigative purposes:
   a. Automated intrusion detection system logs
   b. Firewall logs

c. User account logs
d. Network scanning logs
e. System error logs
f. Application logs
g. Data backup and recovery logs
h. Telephone activity – Call Detail Reports

6. The following audit review may be performed periodically or upon request by assigned technical staff:
   a. Password strength
   b. Unauthorized network devices
   c. Unauthorized personal web servers
   d. Unsecured sharing of devices
   e. Unauthorized modem use
   f. Operating system and software licenses
   g. Unauthorized wireless access points

7. When requested, and for the purpose of performing an audit, any access needed will be provided to members of ESM as designated by the Department's ISM. This access may include:

   a. User level and/or system level access to any computing or communications device
   b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the Department's information resources
   c. Access to work areas that access or process Department information resources
   d. Access to interactively monitor and log traffic on the Department's networks.

8. Any security issues discovered will be reported to the Department's ISM for follow-up review and possible improvement to security settings.

| #B-23: Network Interconnectivity | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #B-23: Network Interconnectivity

### 1.0 Purpose

To ensure that interconnection of External Entities' networks to the Department's networks does not compromise the security of the Department's information resources.

### 2.0 Policy

1. Access to the Department's networks via External Entities' networks shall be protected via firewall or firewall features. No network connection between the Department's network and an external network shall be permitted without the use of firewall features to the appropriate degree based on level of risk, as determined by ISA, in conjunction with the Department's ISM.

2. Access to devices (servers) within the confines of the Department's core network from External Entities' networks shall be limited to the minimum manageable set of users/connections, as determined by ISA in conjunction with the Department's ISM, via firewall features.

3. All External Entities' network connections must meet the requirements of the Florida Information Resource Security Policies and Standards (Rule 74-2). Blanket access is prohibited and the principle of least privilege shall apply. Interconnectivity is limited to services, devices, and equipment needed.

   External Entity Agreements:

   a. All External Entities that desire to connect their networks to the Department's network for the purpose of retrieving Motor Vehicle and Driver License information must complete and submit to the Department the agreement(s) governing External Entity connections.
   b. In addition to the agreement, the External Entity shall be required to submit the Entity's name, address, phone number, fax number, email address, a technical contact's name, phone number, fax number and email address. The Department may request and obtain additional information from the External Entity.
   c. The Department's External Entity connection agreements shall determine the responsibilities of the External Entity, including approval authority levels and all terms and conditions of the agreement.
   d. All External Entities shall implement a binding Memorandum of Understanding, or where applicable, a Management Control Agreement (ex. Entity that manages CJIS data or systems) to ensure appropriate security controls are established and maintained by their trusted partner and agents.

| #B-24: Malware/Virus Protection | Review Date: 08/18/17 | Issue Date: 12/01/08 | Revised Date: 08/18/17 |
|---|---|---|---|

## #B-24: Malware/Virus Protection

### 1.0 Purpose

To ensure the Department's information resources are protected from computer threats, including but not limited to viruses, worms, malware, and other threats of malicious software designed to compromise system confidentiality, integrity, and availability. As a part of the Department's information security program, information resources must receive adequate protection against viruses and malware. External Entities which access and or utilize the Department's information resources are required to adhere to this policy.

### 2.0 Policy

1. All computing devices (workstations, servers, laptops, tablets, etc.) whether connected to the Department's network or storing Department data, must utilize a Department approved virus protection system. The Department's ISM will maintain a list of approved protection vendors. Exceptions to this list will be considered for approval by the Department's ISM on a case-by-case basis.

2. The virus protection system must be enabled on workstations and servers at start-up, employ resident scanning, and never be disabled or bypassed for production usage. The settings for the virus protection system must not be altered in a manner that will reduce the effectiveness of the system.

3. External Entities which access and utilize the Department's information resources are required to update virus signature files immediately upon release.

4. The automatic update frequency of the virus protection system must not be altered to reduce the frequency of updates. Each computing device which accesses Department information resources must utilize a Department approved virus protection system and setup to detect and clean viruses that may infect file shares.

5. External Entities which access or utilize the Department's information resources shall ensure that email is scanned to ensure email and attachments are free from malware and viruses.

6. Each virus, malware, or system exploit that impacts, or potentially impacts the Department's information resources constitutes a security incident and must be reported to the Department's ISM as outlined in #B-10, Incident Handling. The computing device shall be removed from the network until it is verified as free of viruses and malware, and coordinated with the Department's ISM.

| Definitions | Review Date: 08/18/17 | Issue Date: 8/18/17 | Revised Date: 08/18/17 |
|---|---|---|---|

| Term | Definition |
|---|---|
| Access | To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources. |
| Air-Gap | An air gap is a network security measure, also known as air gapping, employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks. |
| Agent | Entity operating on the Department's behalf, but who is not an official Department member. |
| Application Service Provider (ASP) | ASP's combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a Department -owned and operated application. In some cases, systems provided by ASP's reside and operate from within the Department's data center environment. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things. For example: Cloud Provider or Software as a Service Provider. |
| Audit | To examine or verify appropriate use of computing devices and the interconnectivity with External Entities. A Security audit may include **an** independent formal review and examination of system records and activities to (a) determine the adequacy of system controls, (b) ensure compliance with established security policy and operational procedures, (c) detect breaches in security, and (d) recommend any indicated changes in any of the foregoing. |
| Authentication | The process that verifies the claimed identify or access eligibility of a station, originator, or individual as established by an identification process. |
| Authorization | A positive determination by the information resource owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the owner's permission to access the resource. |
| Business Function | The business need that a software application satisfies. Managed by an ASP that hosts an application on behalf of the Department. |
| Chief Information Officer (CIO) | Responsible for the management of the Department's information resources. The Director of Information Systems Administration serves as the Department's CIO. |
| Client | A system that requests and uses the service provided by a "server". |
| Computer security | Measures that implement and assure security in a computer system, particularly those that assure access control; usually understood to include functions, features and technical characteristics of computer hardware and software, especially operating systems. |
| CJIS | Criminal Justice Information Systems. For purposes of this policy, CJIS data and systems process, store, or transmit criminal justice information (CJI). |
| Computing Device | Workstations, servers, laptops, tablets, etc. either connected to the Department's network or which store or process the Department's data. |
| Confidential information | Information that is exempted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Florida Public Records Act. |
| Credentials | The combination of User ID, or Logon ID and password constitute credentials assigned to an entity. |
| Custodian | Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodian is normally a provider of services. |
| Data | A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means. |
| Database | A set of related files that is created and managed by a database management system |
| Denial of service | The prevention of authorized access to a system resource or the delaying of system operations and functions. |
| Department | The Department of Highway Safety and Motor Vehicles. |

| Term | Definition |
|---|---|
| E-mail or email | Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application. |
| Encryption | Encryption is the conversion of data into a form, which cannot be easily understood by unauthorized people. |
| Extranet | Connections between third parties that require access to connections non-public DHSMV resources, as defined in the Network Support Organization's extranet policy. |
| External Entities | Agents, vendors, contractors and consultants who use and/or have access to Department information resources. |
| Firewall | A firewall is a safeguard or type of gateway that is used to control access to information resources. A firewall can control access between separate networks, between network segments, or between a single computer and a network. It can be a PIX, a router with access control lists or similar security devices approved by the Network Support Organization. |
| Host | A computer in a network that provides direct support functions, such as database access, application programs, and programming languages. |
| Incident (or breach) | An event that results in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources whether accidental or deliberate. |
| Information Resources (IR) | For purposes of this policy, information resources are defined as Department owned assets (hardware, systems, software, and data) which are strategic assets vital to the business performance of the Department. |
| Information Security Manager (ISM) | The person designated to administer the Department's information resource security program in accordance with section 282.318(2)(a)1, Florida Statutes, and the Department's internal and external point of contact for all information security matters. |
| Information Systems Administration (ISA) | Entity responsible for computers, networking and data management. |
| Technical Assistance Center (TAC) | The ISA Section that receives requests for assistance from customers using Department computer equipment or network. |
| ISA | Information Systems Administration (within DHSMV). |
| IT (or IR) | Information Technology (or Information Resources). IT is a term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived). |
| Local Area Network (LAN) | Two or more computers and associated devices that share a common communications line within a small geographic area (for example, within an office building), for the purposes of sharing applications, peripherals, data files, etc. |
| Members | Employees of DHSMV. |
| Network | A combination of data circuits and endpoints that are utilized to transmit and receive information. |
| Password | A protected word or string of characters which serves as authentication of a person's identity ("personal password"), or an account identity ("service or system account") which is used to grant or deny access to private or shared data. |
| Physical Security | The protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and damages, whether accidental or intentional. |
| Production or Production System | A system used to process an organization's daily work. It implies a real-time operation and the most mission critical systems in the enterprise. |
| Proprietary Encryption | Encryption technology that has not been made public and/or has not withstood public scrutiny. The developer of the encryption technology could be a vendor, an individual, or the government. |
| Provider | Third party such as a contractor, vendor, or private organization providing products, services and/or support. |

| Term | Definition |
|---|---|
| Remote Desktop Protocol (RDP) | Connection protocol that presents the screen of a remote computing device on a user's computer screen. The user's computer does not have physical access to the external network. The user will be able to use the remote computer as if they were sitting at it. |
| Risk analysis | A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and recommends how to allocate resources to countermeasures so as to minimize total exposure. |
| Security Monitoring | Security monitoring is a process that assists in proactive identification and remediation of security vulnerabilities and threats. This early identification can assist in preventing, or limiting harm to Department information resources. |
| Sensitive Information | Information that is confidential or exempt from disclosure by federal or state law; information that requires protection from unauthorized access by virtue of its legal exemption from the Public Records Act. |
| Server | A physical or virtual computer/device that provides information or services on a network. |
| State | The government of the State of Florida. |
| System Administrator | Person responsible for the effective operation and maintenance of IT, including implementation of standard procedures and controls. |
| Test System | A system that mimics the production environment for the testing of system and application changes yet does not interfere with the production environment. |
| User | An individual who accesses or utilizes the Department's information resources. |
| Virus | A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include data files or the "boot" sector of the hard drive. |
| Wireless Access Point | A wireless receiver, typically 802.1x, which provides connectivity, commonly referred to as "Wi-Fi" from wireless network devices to a wired network. |
| Worm | A worm is a malicious program that can self-replicate and actively transmit itself over a network to infect other computers. |

**CHAPTER 60GG-2**
**INFORMATION TECHNOLOGY SECURITY**



**60GG-2.001 Purpose and Applicability; Definitions**

(1) Purpose and Applicability.

(a) Rules 60GG-2.001 through 60GG-2.006, F.A.C., will be known as the Florida Cybersecurity Standards (FCS).

(b) This rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in rules 60GG-2.001 through 60GG-2.006, F.A.C. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, and the Federal Information Security Management Act of 2002 (44 U.S.C. §3541, et seq.). For the convenience of the reader cross-references to these documents and Special Publications issued by the NIST are provided throughout the FCS as they may be helpful to agencies when drafting their security procedures. The Florida Cybersecurity Standards:

1. Establish minimum standards to be used by state agencies to secure IT resources. The FCS consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risk. The functions identify underlying key categories and subcategories for each function. Subcategories contain specific IT controls. The FCS is visually represented as follows:

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and Access Control |
| | | PR.AT | Awareness & Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes & Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies & Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

Category Unique Identifier subcategory references are detailed in rules 60GG-2.002 – 60GG-2.006, F.A.C., and are used throughout the FCS as applicable.

2. Define minimum management, operational, and technical security controls to be used by state agencies to secure IT resources.

3. Allow authorizing officials to employ compensating security controls or deviate from minimum standards when the agency is unable to implement a security standard or the standard is not cost-effective due to the specific nature of a system or its environment. The agency shall document the reasons why the minimum standards cannot be satisfied and the compensating controls to be employed. After the agency analyzes the issue and related risk a compensating security control or deviation may be employed if the agency documents the analysis and risk steering workgroup accepts the associated risk. This documentation is exempt from section 119.07(1), F.S., pursuant to sections 282.318 (4)(d), and (4)(e), F.S., and, shall be securely submitted to DMS upon acceptance.

(2) Each agency shall:

(a) Perform an assessment that documents the gaps between requirements of this rule and controls that are in place.

(b) Submit the assessment to DMS with the agency's strategic and operational plan.

(c) Reassess annually and update the ASOP to reflect progress toward compliance with this rule.

(3) Definitions.

(a) The following terms are defined:

1. Agency – shall have the same meaning as state agency, as provided in section 282.0041, F.S., except that, per section 282.318(2), F.S., the term also includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

2. Agency-owned (also agency-managed) – any device, service, or technology owned, leased, or managed by the agency for which an agency through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and data management.

3. Authentication – A process of determining the validity of one or more credentials used to claim as digital identity.

4. Authentication protocol – see rule 60GG-5.002, F.A.C.

5. Buyer – refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations.

6. Compensating controls – see rule 60GG-5.001, F.A.C.

7. Complex password – a password sufficiently difficult to correctly guess, which enhances protection of data from unauthorized access. Complexity requires at least eight characters that are a combination of at least three of the following character types: uppercase letters, lowercase letters, numbers, and special characters (@, #, $, %, etc.).

8. Confidential information – records that, pursuant to Florida's public records laws or other controlling law, are exempt from public disclosure.

9. Critical infrastructure – systems and assets, whether physical or virtual so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

10. Critical process – a process that is susceptible to fraud, cyberattack, unauthorized activity, or seriously impacting an agency's mission.

11. Customer – an entity in receipt of services or information rendered by a state agency. This term does not include state agencies with regard to information sharing activities.

12. Cybersecurity event – within the context of rules 60GG-2.001 – 60GG-2.006, F.A.C., a cybersecurity event is a cybersecurity change that may have an impact on agency operations (including mission, capabilities, or reputation).

13. Data-at-rest – stationary data which is stored physically in any digital form.

14. External partners – non-state agency entities doing business with a state agency, including other governmental entities, third parties, contractors, vendors, suppliers and partners. External partners do not include customers.

15. Information Security Manager (ISM) – the person appointed pursuant to section 282.318(4)(a), F.S.

16. Information system owner – the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

17. Industry sector(s) – the following major program areas of state government: Health and Human Services, Education, Government Operations, Criminal and Civil Justice, Agriculture and Natural Resources, and Transportation and Economic

Development.

18. Information technology resources (IT resources) – see section 282.0041(14), F.S.

19. Legacy applications – programs or applications inherited from languages, platforms, and techniques earlier than current technology. These applications may be at or near the end of their useful life but are still required to meet mission objectives or fulfill program area requirements.

20. Mobile Device – any computing device that can be conveniently relocated from one network to another.

21. Multi-Factor Authentication – see rule 60GG-5.001, F.A.C.

22. Personal information – see sections 501.171(1)(g)1., and 817.568, F.S.

23. Privileged user – a user that is authorized (and, therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

24. Privileged accounts – an information system account with authorizations of a privileged user.

25. Remote access – access by users (or information systems) communicating externally to an information security perimeter.

26. Removable Media – any data storage medium or device sufficiently portable to allow for convenient relocation from one network to another.

27. Separation of duties – an internal control concept of having more than one person required to complete a critical process. This is an internal control intended to prevent fraud, abuse, and errors.

28. Stakeholder – a person, group, organization, or state agency involved in or affected by a course of action related to state agency-owned IT resources.

29. Supplier (commonly referred to as "vendor") – encompasses upstream product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided on the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

30. Token control – see rule 60GG-5.001, F.A.C.

31. User – a worker or non-worker who has been provided access to a system or data.

32. Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker).

33. Worker – a member of the workforce. A worker may or may not use IT resources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency.

(b) With the exception of the terms identified in subparagraphs 1.-4., the NIST Glossary of Key Information Security Terms, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (May 2013), maintained at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, is hereby incorporated by reference into this rule: http://www.flrules.org/Gateway/reference.asp?No=Ref-06494.

1. Risk assessment – see section 282.0041(22), F.S.

2. Continuity of Operations Plan (COOP) – disaster-preparedness plans created pursuant to section 252.365(3), F.S.

3. Incident – see section 282.0041(13), F.S.

4. Threat – see section 282.0041(30), F.S.

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.001.*

**60GG-2.002 Identify.**

The identify function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Identify (ID) | Asset Management (AM) | ID.AM-1: Inventory agency physical devices and systems |
| | | ID.AM-2: Inventory agency software platforms and applications |
| | | ID.AM-3: Map agency communication and data flows |
| | | ID.AM-4: Catalog interdependent external information systems |
| | | ID.AM-5: Prioritize IT resources based on classification, criticality, and business value |
| | | ID.AM-6: Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders |

| | | |
|---|---|---|
| | Business Environment (BE) | ID.BE-1: Identify and communicate the agency's role in the business mission/processes |
| | | ID.BE-2: Identify and communicate the agency's place in critical infrastructure and its industry sector to workers |
| | | ID.BE-3: Establish and communicate priorities for agency mission, objectives, and activities |
| | | ID.BE-4: Identify dependencies and critical functions for delivery of critical services |
| | | ID.BE-5: Implement resiliency requirements to support the delivery of critical services for all operating states (e.g., normal operations, under duress, during recovery) |
| | Governance (GV) | ID.GV-1: Establish and communicate an organizational cyber security policy |
| | | ID.GV-2: Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners |
| | | ID.GV-3: Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations |
| | | ID.GV-4: Ensure that governance and risk management processes address cybersecurity risks |
| | Risk Assessment (RA) | ID.RA-1: Identify and document asset vulnerabilities |
| | | ID.RA-2: Receive cyber threat intelligence from information sharing forums and sources |
| | | ID.RA-3: Identify and document threats, both internal and external |
| | | ID.RA-4: Identify potential business impacts and likelihoods |
| | | ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk |
| | | ID.RA-6: Identify and prioritize risk responses |
| | Risk Management Strategy (RM) | ID.RM-1: Establish, manage, and ensure organizational stakeholders understand the approach to be employed via the risk management processes |
| | | ID.RM-2: Determine and clearly express organizational risk tolerance |
| | | ID.RM-3: Ensure that the organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis |
| | Supply Chain Risk Management (SC) | ID.SC-1: Establish management processes to identify, establish, assess, and manage cyber supply chain risk which are agreed to by organizational stakeholders |
| | | ID.SC-2: Identify, prioritize, and assess suppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process |
| | | ID.SC-3: Require suppliers and third-party providers (by contractual requirement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan |
| | | ID.SC-4: Routinely assess suppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers |
| | | ID.SC-5: Conduct response and recovery planning and testing with suppliers and third-party providers |

(1) Asset Management. Each agency shall ensure that IT resources are identified and managed. Identification and management shall be consistent with the IT resource's relative importance to agency objectives and the organization's risk strategy. Specifically, each agency shall:

(a) Ensure that physical devices and systems within the organization are inventoried and managed (ID.AM-1).

(b) Ensure that software platforms and applications within the organization are inventoried and managed (ID.AM-2).

(c) Ensure that organizational communication and data flows are mapped and systems are designed or configured to regulate information flow based on data classification (ID.AM-3). Each agency shall:

1. Establish procedures that ensure only agency-owned or approved IT resources are connected to the agency internal network and resources.

2. Design and document its information security architecture using a defense-in-breadth approach. Design and documentation shall be assessed and updated periodically based on an agency-defined, risk-driven frequency that considers potential threat vectors (i.e., paths or tools that a threat actor may use to attack a target).

3. Consider diverse suppliers when designing the information security architecture.

(d) Each agency shall ensure that interdependent external information systems are catalogued (ID.AM-4). Agencies shall:

1. Verify or enforce required security controls on interconnected external IT resources in accordance with the information security policy or security plan.

2. Implement service level agreements for non-agency provided technology services to ensure appropriate security controls are established and maintained.

3. For non-interdependent external IT resources, execute information sharing or processing agreements with the entity receiving the shared information or hosting the external system in receipt of shared information.

4. Restrict or prohibit portable storage devices either by policy or a technology that enforces security controls for such devices.

5. Authorize and document inter-agency system connections.

6. Require that (e.g., contractually) external service providers adhere to agency security policies.

7. Document agency oversight expectations, and periodically monitor provider compliance.

(e) Each agency shall ensure that IT resources (hardware, data, personnel, devices and software) are categorized, prioritized, and documented based on their classification, criticality, and business value (ID.AM-5). Agencies shall:

1. Perform a criticality analysis for each categorized IT resource and document the findings of the analysis conducted.

2. Designate an authorizing official for each categorized IT resource and document the authorizing official's approval of the security categorization.

3. Create a contingency plan for each categorized IT resource. The contingency plan shall be based on resource classification and identify related cybersecurity roles and responsibilities.

4. Identify and maintain a reference list of exempt, and confidential and exempt agency information or software and the associated applicable state and federal statutes and rules.

(f) Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (ID.AM-6). Each agency is responsible for:

1. Informing workers that they are responsible for safeguarding their passwords and other authentication methods.

2. Informing workers that they shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

3. Informing workers that use, or oversee or manage workers that use, IT equipment that they shall report suspected unauthorized activity, in accordance with agency-established incident reporting procedures.

4. Informing users that they shall take precautions that are appropriate to protect IT resources in their possession from loss, theft, tampering, unauthorized access, and damage. Consideration will be given to the impact that may result if the IT resource is lost, and safety issues relevant to protections identified in this subsection.

5. Informing users of the extent that they will be held accountable for their activities.

6. Informing workers that they have no reasonable expectation of privacy with respect to agency-owned or agency-managed IT resources.

7. Ensuring that monitoring, network sniffing, and related security activities are only to be performed by workers who have been assigned security-related responsibilities either via their approved position descriptions or tasks assigned to them.

8. Appointing an Information Security Manager (ISM). Agency responsibilities related to the ISM include:

a. Notifying the Department of Management Services (DMS) of ISM appointments and reappointments.

b. Specifying ISM responsibilities in the ISM position description.

c. Establishing an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process, including the comprehensive risk assessment required by section 282.318, F.S.; a Computer Security Incident Response Team; and a disaster recovery program that aligns with the agency's Continuity of Operations (COOP) Plan.

d. Each agency ISM shall be responsible for the information security program plan.

9. Performing background checks and ensuring that a background investigation is performed on all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher. See paragraph 60GG-2.002(4)(a), F.A.C. These positions often, if not always, have privileged access. As such, in addition to agency-required background screening, background checks conducted by agencies shall include a federal criminal history check that screens for felony

convictions that concern or involve the following:

a. Computer related or IT crimes;

b. Identity theft crimes;

c. Financially-related crimes, such as: fraudulent practices, false pretenses and frauds, credit card crimes;

d. Forgery and counterfeiting;

e. Violations involving checks and drafts;

f. Misuse of medical or personnel records; and,

g. Theft.

Each agency shall establish appointment selection disqualifying criteria for individuals hired as IT workers that will have access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher.

(2) Business Environment. Each agency's cybersecurity roles, responsibilities, and IT risk management decisions shall align with the agency's mission, objectives, and activities. To accomplish this, agencies shall:

(a) Identify and communicate the agency's role in the business mission of the state (ID.BE-1).

(b) Identify and communicate the agency's place in critical infrastructure and its industry sector to inform internal stakeholders of IT strategy and direction (ID.BE-2).

(c) Establish and communicate priorities for agency mission, objectives, and activities (ID.BE-3).

(d) Identify system dependencies and critical functions for delivery of critical services (ID.BE-4).

(e) Implement information resilience requirements to support the delivery of critical services for all operating states (ID.BE-5).

(3) Governance. Each agency shall establish policies, procedures, and processes to manage and monitor the agency's operational IT requirements based on the agency's assessment of risk. Procedures shall address providing timely notification to management of cybersecurity risks. Agencies shall also:

(a) Establish and communicate a comprehensive cybersecurity policy (ID.GV-1).

(b) Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners (ID.GV-2).

(c) Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations (ID.GV-3).

(d) Ensure governance and risk management processes address cybersecurity risks (ID.GV-4).

(4) Risk Assessment.

(a) Approach. Each agency shall identify and manage the cybersecurity risk to agency operations (including mission, functions, image, or reputation), agency assets, and individuals using the following approach, that derives from the NIST Risk Management Framework (RMF) which may be found at: http://csrc.nist.gov/groups/SMA/fisma/framework.html. The Risk Assessment steps provided in the table below must be followed; however, agencies may identify and, based on the risk to be managed, consider other risk assessment security control requirements and frequency of activities necessary to manage the risk at issue.

| **Risk Assessments** | |
|---|---|
| Categorize: | Categorize information systems and the information processed, stored, and transmitted by that system based on a security impact analysis. |
| Select: | Select baseline security for information systems based on the security categorization; tailoring and supplementing the security baseline as needed based on organization assessment of risk and local conditions. |
| Implement: | Implement the selected baseline security and document how the controls are deployed within information systems and environment of operation. |
| Assess: | Assess the baseline security using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for systems. |
| Authorize: | Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the state resulting from the operation of the information system and the decision that this risk is acceptable. |
| Monitor: | Monitor and assess selected baseline security in information systems on an ongoing basis including assessing control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of systems to appropriate agency officials. |

Agencies are required to consider the following security objectives when assessing risk and determining what kind of assessment is required and when or how often an assessment is to occur: confidentiality, integrity and availability. When determining the potential impact to these security objectives agencies will use the following table, taken from the Federal Information Processing Standards (FIPS) Publication No. 199 (February 2004), which is hereby incorporated into this rule by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06498.

| **POTENTIAL IMPACT** | | | |
|---|---|---|---|
| Security Objectives: | LOW | MODERATE | HIGH |
| **Confidentiality** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability** Ensuring timely and reliable access to and use of information. | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

In accordance with section 282.318(4)(d), F.S., each agency shall complete and submit to DMS no later than July 31, 2017, and every three years thereafter, a comprehensive risk assessment. In completing the risk assessment agencies shall follow the six-step process ("Conducting the Risk Assessment") outlined in Section 3.2 of NIST Special Publication 800-30, utilizing the exemplary tables provided therein as applicable to address that particular agency's threat situation. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1 (September 2012) is hereby incorporated by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06499. When establishing risk management processes, it may be helpful for agencies to review NIST Risk Management Framework Special Publications – they can be downloaded from the following website: http://csrc.nist.gov/publications/PubsSPs.html. When assessing risk, agencies shall estimate the magnitude of harm resulting from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. Estimates shall be documented as low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

(b) Other agency risk management activities that agencies shall perform:

1. Identify and document asset vulnerabilities (ID.RA-1), business processes and protection requirements. Establish procedures to analyze systems and applications to ensure security controls are effective and appropriate.

2. Receive and manage cyber threat intelligence from information sharing forums and sources that contain information relevant to the risks or threats (ID.RA-2).

3. Identify and document internal and external threats (ID.RA-3).

4. Identify potential business impacts and likelihoods (ID.RA-4).

5. Use threats, vulnerabilities, likelihoods, and impacts to determine risk (ID.RA-5).

6. Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation (ID.RA-6).

(5) Risk Management. Each agency shall ensure that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Each agency shall:

(a) Establish risk management processes that are managed and agreed to by agency stakeholders and the agency head (ID.RM-1).

1. Establish a risk steering workgroup that ensures risk management processes are authorized by agency stakeholders. The risk steering workgroup must include a member of the agency IT unit and shall determine the appropriate meeting frequency and agency stakeholders.

(b) Identify and clearly document organizational risk tolerance based on the confidential and exempt nature of the data created, received, maintained, or transmitted by the agency; by the agency's role in critical infrastructure and sector specific analysis (ID.RM-2).

(c) Determine risk tolerance as necessary, based upon: analysis of sector specific risks; the agency's industry sector; agency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for agencies that maintain this information); and the agency's role in the state's mission (ID.RM-3).

(d) Establish parameters for IT staff participation in procurement activities.

(e) Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).

(f) Implement appropriate security controls for software applications obtained, purchased, leased, or developed to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other IT resources.

(g) Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment. Validate that IT resources conform to agency standard configurations prior to implementation into the production environment.

(6) Supply Chain Risk Management. Each agency shall establish priorities, constraints, risk tolerances, and assumptions to support risk decisions associated with managing supply chain risk. Each agency shall:

(a) Establish management processes to identify, establish, assess, and manage cyber supply chain risks which are agreed to by organizational stakeholders (ID.SC-1).

(b) Identify, prioritize, and assess suppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process (ID.SC-2).

(c) Require suppliers and third-party providers (by contractual agreement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan (ID.SC-3).

(d) Routinely assess suppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers (ID.SC-4).

(e) Conduct response and recovery planning and testing with suppliers and third-party providers (ID.SC-5).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-16-16, Amended 2-5-19, Formerly 74-2.002.*

**60GG-2.003 Protect.**

The protect function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Protect (PR) | Identity Management, Authentication, | PR.AC-1: Issue, manage, verify, revoke, and audit identities and credentials for authorized devices, processes, and users |
| | | PR.AC-2: Manage and protect physical access to assets |

| | |
|---|---|
| and Access Control (AC) | PR.AC-3: Manage remote access |
| | PR.AC-4: Manage access permissions and authorizations, incorporate the principles of least privilege and separation of duties |
| | PR.AC-5: Protect network integrity, by incorporating network segregation and segmentation where appropriate |
| | PR.AC-6: Proof and bond identities to credentials, asserting in interactions when appropriate (see token control definition) |
| | PR.AC-7: Authenticate credentials assigned to users, devices, and other assets commensurate with the risk of the transaction. |
| Awareness and Training (AT) | PR.AT-1: Inform and train all users |
| | PR.AT-2: Ensure that privileged users understand roles and responsibilities |
| | PR.AT-3: Ensure that third-party stakeholders understand roles and responsibilities |
| | PR.AT-4: Ensure that senior executives understand roles and responsibilities |
| | PR.AT-5: Ensure that physical and cybersecurity personnel understand their roles and responsibilities |
| Data Security (DS) | PR.DS-1: Protect data-at-rest |
| | PR.DS-2: Protect data-in-transit |
| | PR.DS-3: Formally manage assets managed throughout removal, transfers, and disposition |
| | PR.DS-4: Ensure that adequate capacity is maintained to support availability needs |
| | PR.DS-5: Implement data leak protection measures |
| | PR.DS-6: Use integrity checking mechanisms to verify software, firmware, and information integrity |
| | PR.DS-7: Logically or physically separate the development and testing environment(s) from the production environment |
| | PR.DS-8: Use integrity checking mechanisms to verify hardware integrity |
| Information Protection Processes and Procedures | PR.IP-1: Create and maintain a baseline configuration that incorporates all security principles for information technology/industrial control systems |
| | PR.IP-2: Implement a System Development Life Cycle (SDLC) to manage systems |
| | PR.IP-3: Establish configuration change control processes |
| | PR.IP-4: Conduct, maintain, and test backups of information |
| | PR.IP-5: Meet policy and regulatory requirements that are relevant to the physical operating environment for organizational assets |
| | PR.IP-6: Destroy data according to policy |
| | PR.IP-7: Continuously improve protection processes |
| | PR.IP-8: Share effectiveness of protection technologies with stakeholders that should or must receive this information |
| | PR.IP-9: Establish and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) |
| | PR.IP-10: Test response and recovery plans |
| | PR.IP-11: Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening) |
| | PR.IP-12: Develop and implement a vulnerability management plan |
| Maintenance (MA) | PR.MA-1: Perform and log maintenance and repair of organizational assets, with approved and controlled tools |
| | PR.MA-2: Approve, log, and perform remote maintenance of agency assets in a manner that prevents unauthorized access |
| Protective Technology | PR.PT-1: Determine, document, implement, and review audit/log records in accordance with policy |

| | | |
|---|---|---|
| | (PT) | PR.PT-2: Protect and restrict removable media usage according to policy |
| | | PR.PT-3: Incorporate the principle of least functionality by configuring systems to provide only essential capabilities |
| | | PR.PT-4: Protect communications and control networks |
| | | PR.PT-5: Implement mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations |

(1) Access Control. Each agency shall ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Specifically:

(a) Each agency shall manage identities and credentials for authorized devices and users (PR.AC-1). Control measures shall, at a minimum include authentication token(s) unique to the individual.

Agencies shall:

1. Require that all agency-owned or approved computing devices, including mobile devices, use unique user authentication.

2. Require users to log off or lock their workstations prior to leaving the work area.

3. Require inactivity timeouts that log-off or lock workstations or sessions.

4. Locked workstations or sessions must be locked in a way that requires user authentication with an authentication token(s) unique to the individual user to disengage.

5. When passwords are used as the sole authentication token, require users to use complex passwords that are changed at least every 90 days.

6. Address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations and facilitate periodic review of access rights with information owners. Frequency of reviews shall be based on system categorization or assessed risk.

7. Establish access disablement and notification timeframes for worker separations. The agency will identify the appropriate person in the IT unit to receive notification. Notification timeframes shall consider risks associated with system access post-separation.

8. Ensure IT access is removed when the IT resource is no longer required.

9. Require MFA for access to networks or applications that have a categorization of moderate, high, or contain exempt, or confidential and exempt, information. This excludes externally hosted systems designed to deliver services to agency customers where the agency documents the analysis and the risk steering workgroup accepts the associated risk.

10. Require MFA for access to privileged accounts.

(b) Each agency shall manage and protect physical access to assets (PR.AC-2). In doing so, agency security procedures or controls shall:

1. Address protection of IT resources from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturer specifications.

2. Implement procedures to manage physical access to IT facilities and/or equipment.

3. Identify physical controls that are appropriate for the size and criticality of the IT resources.

4. Specify physical access to information resource facilities and/or equipment that is restricted to authorized personnel.

5. Detail visitor access protocols, including recordation procedures, and in locations housing systems categorized as moderate-impact or high-impact, require that visitors be supervised by authorized personnel.

6. Address how the agency will protect network integrity by incorporating network segregation.

(c) Each agency shall manage remote access (PR.AC-3). In doing so, agencies shall:

1. Address how the agency will securely manage and document remote access.

2. Specify that only secure, agency-managed, remote access methods may be used to remotely connect computing devices to the agency internal network.

3. For systems containing exempt, or confidential and exempt data, ensure written agreements and procedures are in place to ensure security for sharing, handling or storing confidential data with entities outside the agency.

(d) Each agency shall ensure that access permissions and authorizations, are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4). In doing so, agencies shall:

1. Execute interconnection security agreements to authorize, document, and support continual management of inter-agency connected systems.

2. Manage access permissions by incorporating the principles of “least privilege” and “separation of duties.”

3. Specify that all workers be granted access to agency IT resources based on the principles of “least privilege” and “need to know determination.”

4. Specify that system administrators restrict and tightly control the use of system development utility programs that may be capable of overriding system and application controls.

(e) Each agency shall ensure that network integrity is protected, incorporating network segregation and segmentation where appropriate (PR.AC-5).

(f) Proof and bond identities to credentials and assert in interactions when appropriate (PR.AC-6).

(g) Authenticate users, devices, and other assets commensurate with the risk of the transaction (PR.AC-7).

(2) Awareness and Training. Agencies shall provide all their workers cybersecurity awareness education and training so as to ensure they perform their cybersecurity related duties and responsibilities consistent with agency policies and procedures. In doing so, each agency shall:

(a) Inform and train all workers (PR.AT-1).

(b) Ensure that privileged users understand their roles and responsibilities (PR.AT-2).

(c) Ensure that third-party stakeholders understand their roles and responsibilities (PR.AT-3).

(d) Ensure that senior executives understand their roles and responsibilities (PR.AT-4).

(e) Ensure that physical and cybersecurity personnel understand their roles and responsibilities (PR.AT-5).

(3) For each of the above subsections the following shall also be addressed:

(a) Appoint a worker to coordinate the agency information security awareness program. If an IT security worker does not coordinate the security awareness program, they shall be consulted for content development purposes. Agencies will ensure that all workers (including volunteer workers) are clearly notified of applicable obligations, established via agency policies, to maintain compliance with such controls.

(b) Establish a program that includes, at a minimum, annual security awareness training and on-going education and reinforcement of security practices.

(c) Provide training to workers within 30 days of start date.

(d) Include security policy adherence expectations for the following, at a minimum: disciplinary procedures and implications, acceptable use restrictions, data handling (procedures for handling exempt and confidential and exempt information), telework and cybersecurity incident reporting procedures. Incident reporting procedures shall:

1. Establish requirements for workers to immediately report loss of mobile devices, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency reporting procedures.

(e) Where technology permits, provide training prior to system access. For specialized agency workers (e.g., law enforcement officers) who are required to receive extended off-site training prior to reporting to their permanent duty stations, initial security awareness training shall be provided within 30 days of the date they report to their permanent duty station.

(f) Require, prior to access, workers verify in writing that they will comply with agency IT security policies and procedures.

(g) Document parameters that govern personal use of agency IT resources and define what constitutes personal use. Personal use, if allowed by the agency, shall not interfere with the normal performance of any worker’s duties, or consume significant or unreasonable amounts of state IT resources (e.g., bandwidth, storage).

(h) Inform workers of what constitutes inappropriate use of IT resources. Inappropriate use shall include, but may not be limited to, the following:

1. Distribution of malware.

2. Disablement or circumvention of security controls.

3. Forging headers.

4. Political campaigning or unauthorized fundraising.

5. Use for personal profit, benefit or gain.

6. Offensive, indecent, or obscene access or activities, unless required by job duties.

7. Harassing, threatening, or abusive activity.

8. Any activity that leads to performance degradation.

9. Auto-forwarding to external email addresses.

10. Unauthorized, non-work-related access to: chat rooms, political groups, singles clubs or dating services; peer-to-peer file

sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker web-site/software; and pornography and sites containing obscene materials.

(4) Data Security. Each agency shall manage and protect records and data, including data-at-rest, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Agencies shall establish procedures, and develop and maintain agency cryptographic implementations. Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, and prevention of unauthorized substitution. Also, key management processes must be in place and verified prior to encrypting data at rest, to prevent data loss and support availability. In protecting data security, agencies shall:

(a) Protect data-at-rest by establishing (PR.DS-1):

1. Procedures that ensure only agency-owned or approved IT resources are used to store confidential or exempt information.

2. Procedures that ensure agency-owned or approved portable IT resources containing confidential or mission critical data are encrypted.

3. Procedures that ensure agency-owned or approved portable IT resources that connect to the agency internal network use agency-managed security software.

4. Inform users not to store unique copies of agency data on workstations or mobile devices.

(b) Protect data-in-transit (PR.DS-2). Each agency shall:

1. Encrypt confidential and exempt information during transmission, except when the transport medium is owned or managed by the agency and controls are in place to protect the data during transit.

2. Ensure that wireless transmissions of agency data employ cryptography for authentication and transmission.

3. Make passwords unreadable during transmission and storage.

4. Encrypt mobile IT resources that store, process, or transmit exempt, or confidential and exempt agency data.

(c) Formally manage assets throughout removal, transfer, and disposition (PR.DS-3).

1. Ensure any records stored on storage media to be disposed of or released for reuse, are sanitized or destroyed in accordance with organization-developed procedures and the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.

2. Destruction of confidential or exempt information shall be conducted such that the information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.

3. Document procedures for sanitization of agency-owned IT resources prior to reassignment or disposal.

4. Equipment sanitization shall be performed such that confidential or exempt information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction. File deletion and media formatting are not acceptable methods of sanitization. Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

(d) Maintain adequate capacity to ensure system availability and data integrity (PR.DS-4).

1. Ensure adequate audit/log capacity.

2. Protect against or limit the effects of denial of service attacks.

(e) Implement protections against data leaks or unauthorized data disclosures by establishing policies and procedures that address (PR.DS-5):

1. Appropriate handling and protection of exempt, and confidential and exempt, information. Policies shall be reviewed and acknowledged by all workers.

2. Retention and destruction of confidential and exempt information in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.

3. Access agreements for agency information systems.

4. Boundary protection.

5. Transmission confidentiality and integrity.

(f) Employ integrity checking mechanisms to verify software, firmware, and information integrity (PR.DS-6).

1. Application controls shall be established to ensure the accuracy and completeness of data, including validation and integrity checks, to detect data corruption that may occur through processing errors or deliberate actions.

(g) Physically or logically separate development and testing environment(s) from the production environment and ensure that

production exempt, or confidential and exempt data is not used for development where technology permits. Production exempt, or confidential and exempt data may be used for testing if the data owner authorizes the use and regulatory prohibitions do not exist; the test environment limits access and access is audited; and production exempt, and confidential and exempt data is removed from the system when testing is completed. Data owner authorization shall be managed via technical means, to the extent practical (PR.DS-7).

(h) Use integrity checking mechanisms to verify hardware integrity (PR.DS-8). In doing so, agencies shall establish processes to protect against and/or detect unauthorized changes to hardware used to support systems with a categorization of high-impact.

(5) Information Protection Processes and Procedures. Each agency shall ensure that security policies, processes and procedures are maintained and used to manage protection of information systems and assets. Such policies, processes and procedures shall:

(a) Include a current baseline configuration of information systems which incorporate security principles (PR.IP-1). Baselines shall:

1. Specify standard hardware and secure standard configurations.

2. Include documented firewall and router configuration standards, and include a current network diagram.

3. Require that vendor default settings, posing security risks, are changed or disabled for agency-owned or managed IT resources, including encryption keys, accounts, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure device security settings are enabled where appropriate.

4. Allow only agency-approved software to be installed on agency-owned IT resources.

(b) Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2). In doing so, agencies shall:

1. Develop and implement processes that include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

2. Ensure security reviews are approved by the ISM and Chief Information Officer (or designee) before new or modified applications or technologies are moved into production. For IT resources housed in a state data center, the security review shall also be approved by the data center before the new or modified applications or technologies are moved into production.

3. The application development team at each agency shall implement appropriate security controls to minimize risks to agency IT resources and meet the security requirements of the application owner. Agencies will identify in their policies, processes and procedures the security coding guidelines the agency will follow when obtaining, purchasing, leasing or developing software.

4. Where technology permits, the agency shall ensure anti-malware software is maintained on agency IT resources.

(c) Establish a configuration change control process to manage upgrades and modifications to existing IT resources (PR.IP-3). In doing so, agencies shall:

1. Determine types of changes that are configuration-controlled (e.g. emergency patches, releases, and other out-of-band security packages).

2. Develop a process to review and approve or disapprove proposed changes based on a security impact analysis (e.g., implementation is commensurate with the risk associated with the weakness or vulnerability).

3. Develop a process to document change decisions.

4. Develop a process to implement approved changes and review implemented changes.

5. Develop an oversight capability for change control activities.

6. Develop procedures to ensure security requirements are incorporated into the change control process.

(d) Ensure backups of information are conducted, maintained, and tested (PR.IP-4).

(e) Establish policy and regulatory expectations for protection of the physical operating environment for agency-owned or managed IT resources (PR.IP-5).

(f) Manage and dispose of records/data in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies (PR.IP-6).

(g) Establish a policy and procedure review process that facilitates continuous improvement to protection processes (PR.IP-7). Each agency shall:

1. Ensure system security control selection occurs during the beginning of the SDLC and is documented in final design documentation.

2. Ensure system security plans shall document controls necessary to protect production data in the production environment and copies of production data used in non-production environments.

3. Ensure system security plans are confidential per section 282.318, F.S., and shall be available to the agency ISM.

4. Require that each agency application or system with a categorization of moderate-impact or higher have a documented system security plan (SSP). For existing production systems that lack a SSP, a risk assessment shall be performed to determine prioritization of subsequent documentation efforts. The SSP shall include provisions that:

(I) Align the system with the agency's enterprise architecture.

(II) Define the authorization boundary for the system.

(III) Describe the mission-related business purpose.

(IV) Provide the security categorization, including security requirements and rationale (compliance, availability, etc.).

(V) Describe the operational environment, including relationships, interfaces, or dependencies on external services.

(VI) Provide an overview of system security requirements.

(VII) Identify authorizing official or designee, who reviews and approves prior to implementation.

5. Require information system owners (ISOs) to define application security-related business requirements using role-based access controls and rule-based security policies where technology permits.

6. Require ISOs to establish and authorize the types of privileges and access rights appropriate to system users, both internal and external.

7. Create procedures to address inspection of content stored, processed or transmitted on agency-owned or managed IT resources, including attached removable media. Inspection shall be performed where authorization has been provided by stakeholders that should or must receive this information.

8. Establish parameters for agency-managed devices that prohibit installation (without worker consent) of clients that allow the agency to inspect private partitions or personal data.

9. Require ISOs ensure segregation of duties when establishing system authorizations.

10. Establish controls that prohibit a single individual from having the ability to complete all steps in a transaction or control all stages of a critical process.

11. Require agency information owners to identify exempt, and confidential and exempt information in their systems.

(h) Ensure that effectiveness of protection technologies is shared with stakeholders that should or must receive this information (PR.IP-8).

(i) Develop, implement and manage response plans (e.g., Incident Response and Business Continuity) and recovery plans (e.g., Incident Recovery and Disaster Recovery) (PR.IP-9).

(j) Establish a procedure that ensures that agency response and recovery plans are regularly tested (PR.IP-10).

(k) Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening) (PR.IP-11).

(l) Each agency shall develop and implement a vulnerability management plan (PR.IP-12).

(6) Maintenance. Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures. Each agency shall:

(a) Perform and log maintenance and repair of IT resources, with tools that have been approved and are administered by the agency to be used for such activities (PR.MA-1).

(b) Approve, encrypt, log and perform remote maintenance of IT resources in a manner that prevents unauthorized access (PR.MA-2).

(c) Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing agency-developed authenticators in legacy applications.

(7) Protective Technology. Each agency shall ensure that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Specifically, each agency shall:

(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with agency-developed policy. Agency-developed policy shall be based on resource criticality. Where possible, ensure that electronic audit records allow actions of users to be uniquely traced to those users so they can be held accountable for their actions. Maintain logs identifying where access to exempt, or confidential and exempt data was permitted. The logs shall support unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed or transmitted by the individual (PR.PT-1).

(b) Protect and restrict removable media in accordance with agency-developed information security policy (PR.PT-2).

(c) Incorporate the principle of least functionality by configuring systems to only provide essential capabilities (PR.PT-3).

(d) Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources (PR.PT-4). Agencies shall:

1. Place databases containing mission critical, exempt, or confidential and exempt data in an internal network zone, segregated from the demilitarized zone (DMZ).

2. Agencies shall require host-based (e.g., a system controlled by a central or main computer) boundary protection on mobile computing devices where technology permits (i.e., detection agent).

(e) Implement mechanisms (e.g., failsafe, load balancing across duplicated systems, hot swap) to achieve resilience requirements in normal and adverse situations (PR.PT-5).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.003.*

**60GG-2.004 Detect.**

The detect function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Detect (DE) | Anomalies and Events (AE) | DE.AE-1: Establish and manage a baseline of network operations and expected data flows for users and systems |
| | | DE.AE-2: Analyze detected cybersecurity events to understand attack targets and methods |
| | | DE.AE-3: Collect and correlate cybersecurity event data from multiple sources and sensors |
| | | DE.AE-4: Determine the impact of cybersecurity events |
| | | DE.AE-5: Establish incident alert thresholds |
| | Security Continuous Monitoring (CM) | DE.CM-1: Monitor the network to detect potential cybersecurity events |
| | | DE.CM-2: Monitor the physical environment to detect potential cybersecurity events |
| | | DE.CM-3: Monitor personnel activity to detect potential cybersecurity events |
| | | DE.CM-4: Detect malicious code |
| | | DE.CM-5: Detect unauthorized mobile code |
| | | DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events |
| | | DE.CM-7: Monitor for unauthorized personnel, connections, devices, and software |
| | | DE.CM-8: Perform vulnerability scans |
| | Detection Processes (DP) | DE.DP-1: Define roles and responsibilities for detection to ensure accountability |
| | | DE.DP-2: Ensure that detection activities comply with all applicable requirements |
| | | DE.DP-3: Test detection processes |
| | | DE.DP-4: Communicate event detection information to stakeholders that should or must receive this information |
| | | DE.DP-5: Continuously improve detection processes |

(1) Anomalies and Events. Each agency shall develop policies and procedures that will facilitate detection of anomalous activity and that allow the agency to understand the potential impact of events.

Such policies and procedures shall:

(a) Establish and manage a baseline of network operations and expected data flows for users and systems (DE.AE-1).

(b) Detect and analyze anomalous cybersecurity events to determine attack targets and methods (DE.AE-2).

1. Monitor for unauthorized wireless access points connected to the agency internal network, and immediately remove them upon detection.

2. Implement procedures to establish accountability for accessing and modifying exempt, or confidential and exempt, data stores to ensure inappropriate access or modification is detectable.

(c) Collect and correlate cybersecurity event data from multiple sources and sensors (DE.AE-3).

(d) Determine the impact of cybersecurity events (DE.AE-4).

(e) Establish incident alert thresholds (DE.AE-5).

(2) Security Continuous Monitoring. Each agency shall determine the appropriate level of monitoring that will occur regarding IT resources necessary to identify cybersecurity events and verify the effectiveness of protective measures. Such activities shall

include:

(a) Monitoring the network to detect potential cybersecurity events (DE.CM-1).

(b) Monitoring for unauthorized IT resource connections to the internal agency network.

(c) Monitoring the physical environment to detect potential cybersecurity events (DE.CM-2).

(d) Monitoring user activity to detect potential cybersecurity events (DE.CM-3).

(e) Monitoring for malicious code (DE.CM-4).

(f) Monitoring for unauthorized mobile code (DE.CM-5).

(g) Monitoring external service provider activity to detect potential cybersecurity events (DE.CM-6).

(h) Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7).

(i) Performing vulnerability scans (DE.CM-8). These shall be a part of the System Development Life Cycle (SDLC).

(3) Detection Processes. Each agency shall maintain and test detection processes and procedures to ensure awareness of anomalous events. These procedures shall be based on assigned risk and include the following:

(a) Defining roles and responsibilities for detection to ensure accountability (DE.DP-1).

(b) Ensuring that detection activities comply with all applicable requirements (DE.DP-2).

(c) Testing detection processes (DE.DP-3).

(d) Communicating event detection information to stakeholders that should or must receive this information (DE.DP-4).

(e) Continuously improving detection processes (DE.DP-5).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.004.*

**60GG-2.005 Respond.**

The respond function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Respond (RS) | Response Planning (RP) | RS.RP-1: Execute response plan during or after an incident |
| | Communications (CO) | RS.CO-1: Ensure that personnel know their roles and order of operations when a response is needed |
| | | RS.CO-2: Report incidents consistent with established criteria |
| | | RS.CO-3: Share information consistent with response plans |
| | | RS.CO-4: Coordinate with stakeholders consistent with response plans |
| | | RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness |
| | Analysis (AN) | RS.AN-1: Investigate notifications from detection systems |
| | | RS.AN-2: Understand the impact of incidents |
| | | RS.AN-3: Perform forensic analysis |
| | | RS.AN-4: Categorize incidents consistent with response plans |
| | | RS.AN-5: Establish processes to receive, analyze, and respond to vulnerabilities disclosed to the agency from internal and external sources |
| | Mitigation (MI) | RS.MI-1: Contain incidents |
| | | RS.MI-2: Mitigate incidents |
| | | RS.MI-3: Mitigate newly identified vulnerabilities or document accepted risks |
| | Improvements (IM) | RS.IM-1: Incorporate lessons learned in response plans |
| | | RS.IM-2: Periodically update response strategies |

(1) Response Planning. Each agency shall establish and maintain response processes and procedures and validate execution capability to ensure agency response for detected cybersecurity incidents. Each agency shall execute a response plan during or after an incident (RS.RP-1).

(a) Agencies shall establish a Computer Security Incident Response Team (CSIRT) to respond to cybersecurity incidents. CSIRT members shall convene immediately, upon notice of cybersecurity incidents. Responsibilities of CSIRT members include:

1. Convening a simple majority of CSIRT members at least quarterly to review, at a minimum, established processes and

escalation protocols.

2. Receiving incident response training annually. Training shall be coordinated as a part of the information security program.

3. CSIRT membership shall include, at a minimum, a member from the information security team, the CIO (or designee), and a member from the Inspector General's Office who shall act in an advisory capacity. The CSIRT team shall report findings to agency management.

4. The CSIRT shall determine the appropriate response required for each cybersecurity incident.

5. The agency security incident reporting process must include notification procedures, established pursuant to section 501.171, F.S., section 282.318, F.S., and as specified in executed agreements with external parties. For reporting incidents to DMS and the Cybercrime Office (as established within the Florida Department of Law Enforcement via section 943.0415, F.S.), agencies shall report observed incident indicators via the DMS Incident Reporting Portal to provide early warning and proactive response capability to other State of Florida agencies. Such indicators may include any known attacker IP addresses, malicious uniform resource locator (URL) addresses, malicious code file names and/or associated file hash values.

(2) Communications. Each agency shall coordinate response activities with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. Each agency shall:

(a) Inform workers of their roles and order of operations when a response is needed (RS.CO-1).

(b) Require that incidents be reported consistent with established criteria and in accordance with agency incident reporting procedures. Criteria shall require immediate reporting, including instances of lost identification and authentication resources (RS.CO-2).

(c) Share information, consistent with response plans (RS.CO-3).

(d) Coordinate with stakeholders, consistent with response plans (RS.CO-4).

(e) Establish communications with external stakeholders to share and receive information to achieve broader cybersecurity situational awareness (RS.CO-5). Where technology permits, enable automated security alerts. Establish processes to receive, assess, and act upon security advisories.

(3) Analysis. Each agency shall conduct analysis to adequately respond and support recovery activities. Related activities include:

(a) Each agency shall establish notification thresholds and investigate notifications from detection systems (RS.AN-1).

(b) Each agency shall assess and identify the impact of incidents (RS.AN-2).

(c) Each agency shall perform forensics, where deemed appropriate (RS.AN-3).

(d) Each agency shall categorize incidents, consistent with response plans (RS.AN-4). Each incident report and analysis, including findings and corrective actions, shall be documented.

(e) Establish processes to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (RS.AN-5).

(4) Mitigation. Each agency shall perform incident mitigation activities. The objective of incident mitigation activities shall be to: attempt to contain and prevent recurrence of incidents (RS.MI-1); mitigate incident effects and resolve the incident (RS.MI-2); and address vulnerabilities or document as accepted risks.

(5) Improvements. Each agency shall improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into response plans (RS.IM-1). Agencies shall update response strategies in accordance with agency-established policy (RS.IM-2).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.005.*

**60GG-2.006 Recover.**

The recover function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Recover (RC) | Recovery Planning (RP) | RC.RP-1: Execute recovery plan during or after a cybersecurity incident |
| | Improvements (IM) | RC.IM-1: Incorporate lessons learned in recovery plans |
| | | RC.IM-2: Periodically update recovery strategies |
| | Communications (CO) | RC.CO-1: Manage public relations |
| | | RC.CO-2: Repair reputation after an event |

| | | |
|---|---|---|
| | | RC.CO-3: Communicate recovery activities to internal stakeholders and executive and management teams |

(1) Recovery Planning. Each agency shall execute and maintain recovery processes and procedures to ensure restoration of systems or assets affected by cybersecurity incidents. Each agency shall:

(a) Execute a recovery plan during or after an incident (RC.RP-1).

(b) Mirror data and software, essential to the continued operation of critical agency functions, to an off-site location or regularly back up a current copy and store at an off-site location.

(c) Develop procedures to prevent loss of data, and ensure that agency data, including unique copies, are backed up.

(d) Document disaster recovery plans that address protection of critical IT resources and provide for the continuation of critical agency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical agency functions.

(e) IT disaster recovery plans shall be tested at least annually; results of the annual exercise shall document plan procedures that were successful and specify any modifications required to improve the plan.

(2) Improvements. Each agency shall improve recovery planning and processes by incorporating lessons learned into future activities. Such activities shall include:

(a) Incorporating lessons learned in recovery plans (RC.IM-1).

(b) Updating recovery strategies (RC.IM-2).

(3) Communications. Each agency shall coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Such activities shall include:

(a) Managing public relations (RC.CO-1).

(b) Attempts to repair reputation after an event, if applicable (RC.CO-2).

(c) Communicating recovery activities to stakeholders, internal and external where appropriate (RC.CO-3).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.006.*

**CHAPTER 60GG-2**
**INFORMATION TECHNOLOGY SECURITY**



**60GG-2.001 Purpose and Applicability; Definitions**

(1) Purpose and Applicability.

(a) Rules 60GG-2.001 through 60GG-2.006, F.A.C., will be known as the Florida Cybersecurity Standards (FCS).

(b) This rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in rules 60GG-2.001 through 60GG-2.006, F.A.C. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, and the Federal Information Security Management Act of 2002 (44 U.S.C. §3541, et seq.). For the convenience of the reader cross-references to these documents and Special Publications issued by the NIST are provided throughout the FCS as they may be helpful to agencies when drafting their security procedures. The Florida Cybersecurity Standards:

1. Establish minimum standards to be used by state agencies to secure IT resources. The FCS consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risk. The functions identify underlying key categories and subcategories for each function. Subcategories contain specific IT controls. The FCS is visually represented as follows:

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and Access Control |
| | | PR.AT | Awareness & Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes & Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies & Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

Category Unique Identifier subcategory references are detailed in rules 60GG-2.002 – 60GG-2.006, F.A.C., and are used throughout the FCS as applicable.

2. Define minimum management, operational, and technical security controls to be used by state agencies to secure IT resources.

3. Allow authorizing officials to employ compensating security controls or deviate from minimum standards when the agency is unable to implement a security standard or the standard is not cost-effective due to the specific nature of a system or its environment. The agency shall document the reasons why the minimum standards cannot be satisfied and the compensating controls to be employed. After the agency analyzes the issue and related risk a compensating security control or deviation may be employed if the agency documents the analysis and risk steering workgroup accepts the associated risk. This documentation is exempt from section 119.07(1), F.S., pursuant to sections 282.318 (4)(d), and (4)(e), F.S., and, shall be securely submitted to DMS upon acceptance.

(2) Each agency shall:

(a) Perform an assessment that documents the gaps between requirements of this rule and controls that are in place.

(b) Submit the assessment to DMS with the agency's strategic and operational plan.

(c) Reassess annually and update the ASOP to reflect progress toward compliance with this rule.

(3) Definitions.

(a) The following terms are defined:

1. Agency – shall have the same meaning as state agency, as provided in section 282.0041, F.S., except that, per section 282.318(2), F.S., the term also includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

2. Agency-owned (also agency-managed) – any device, service, or technology owned, leased, or managed by the agency for which an agency through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and data management.

3. Authentication – A process of determining the validity of one or more credentials used to claim as digital identity.

4. Authentication protocol – see rule 60GG-5.002, F.A.C.

5. Buyer – refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations.

6. Compensating controls – see rule 60GG-5.001, F.A.C.

7. Complex password – a password sufficiently difficult to correctly guess, which enhances protection of data from unauthorized access. Complexity requires at least eight characters that are a combination of at least three of the following character types: uppercase letters, lowercase letters, numbers, and special characters (@, #, $, %, etc.).

8. Confidential information – records that, pursuant to Florida's public records laws or other controlling law, are exempt from public disclosure.

9. Critical infrastructure – systems and assets, whether physical or virtual so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

10. Critical process – a process that is susceptible to fraud, cyberattack, unauthorized activity, or seriously impacting an agency's mission.

11. Customer – an entity in receipt of services or information rendered by a state agency. This term does not include state agencies with regard to information sharing activities.

12. Cybersecurity event – within the context of rules 60GG-2.001 – 60GG-2.006, F.A.C., a cybersecurity event is a cybersecurity change that may have an impact on agency operations (including mission, capabilities, or reputation).

13. Data-at-rest – stationary data which is stored physically in any digital form.

14. External partners – non-state agency entities doing business with a state agency, including other governmental entities, third parties, contractors, vendors, suppliers and partners. External partners do not include customers.

15. Information Security Manager (ISM) – the person appointed pursuant to section 282.318(4)(a), F.S.

16. Information system owner – the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

17. Industry sector(s) – the following major program areas of state government: Health and Human Services, Education, Government Operations, Criminal and Civil Justice, Agriculture and Natural Resources, and Transportation and Economic

Development.

18. Information technology resources (IT resources) – see section 282.0041(14), F.S.

19. Legacy applications – programs or applications inherited from languages, platforms, and techniques earlier than current technology. These applications may be at or near the end of their useful life but are still required to meet mission objectives or fulfill program area requirements.

20. Mobile Device – any computing device that can be conveniently relocated from one network to another.

21. Multi-Factor Authentication – see rule 60GG-5.001, F.A.C.

22. Personal information – see sections 501.171(1)(g)1., and 817.568, F.S.

23. Privileged user – a user that is authorized (and, therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

24. Privileged accounts – an information system account with authorizations of a privileged user.

25. Remote access – access by users (or information systems) communicating externally to an information security perimeter.

26. Removable Media – any data storage medium or device sufficiently portable to allow for convenient relocation from one network to another.

27. Separation of duties – an internal control concept of having more than one person required to complete a critical process. This is an internal control intended to prevent fraud, abuse, and errors.

28. Stakeholder – a person, group, organization, or state agency involved in or affected by a course of action related to state agency-owned IT resources.

29. Supplier (commonly referred to as "vendor") – encompasses upstream product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided on the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

30. Token control – see rule 60GG-5.001, F.A.C.

31. User – a worker or non-worker who has been provided access to a system or data.

32. Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker).

33. Worker – a member of the workforce. A worker may or may not use IT resources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency.

(b) With the exception of the terms identified in subparagraphs 1.-4., the NIST Glossary of Key Information Security Terms, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (May 2013), maintained at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, is hereby incorporated by reference into this rule: http://www.flrules.org/Gateway/reference.asp?No=Ref-06494.

1. Risk assessment – see section 282.0041(22), F.S.

2. Continuity of Operations Plan (COOP) – disaster-preparedness plans created pursuant to section 252.365(3), F.S.

3. Incident – see section 282.0041(13), F.S.

4. Threat – see section 282.0041(30), F.S.

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.001.*

**60GG-2.002 Identify.**

The identify function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Identify (ID) | Asset Management (AM) | ID.AM-1: Inventory agency physical devices and systems |
| | | ID.AM-2: Inventory agency software platforms and applications |
| | | ID.AM-3: Map agency communication and data flows |
| | | ID.AM-4: Catalog interdependent external information systems |
| | | ID.AM-5: Prioritize IT resources based on classification, criticality, and business value |
| | | ID.AM-6: Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders |

| | | |
|---|---|---|
| | Business Environment (BE) | ID.BE-1: Identify and communicate the agency's role in the business mission/processes |
| | | ID.BE-2: Identify and communicate the agency's place in critical infrastructure and its industry sector to workers |
| | | ID.BE-3: Establish and communicate priorities for agency mission, objectives, and activities |
| | | ID.BE-4: Identify dependencies and critical functions for delivery of critical services |
| | | ID.BE-5: Implement resiliency requirements to support the delivery of critical services for all operating states (e.g., normal operations, under duress, during recovery) |
| | Governance (GV) | ID.GV-1: Establish and communicate an organizational cyber security policy |
| | | ID.GV-2: Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners |
| | | ID.GV-3: Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations |
| | | ID.GV-4: Ensure that governance and risk management processes address cybersecurity risks |
| | Risk Assessment (RA) | ID.RA-1: Identify and document asset vulnerabilities |
| | | ID.RA-2: Receive cyber threat intelligence from information sharing forums and sources |
| | | ID.RA-3: Identify and document threats, both internal and external |
| | | ID.RA-4: Identify potential business impacts and likelihoods |
| | | ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk |
| | | ID.RA-6: Identify and prioritize risk responses |
| | Risk Management Strategy (RM) | ID.RM-1: Establish, manage, and ensure organizational stakeholders understand the approach to be employed via the risk management processes |
| | | ID.RM-2: Determine and clearly express organizational risk tolerance |
| | | ID.RM-3: Ensure that the organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis |
| | Supply Chain Risk Management (SC) | ID.SC-1: Establish management processes to identify, establish, assess, and manage cyber supply chain risk which are agreed to by organizational stakeholders |
| | | ID.SC-2: Identify, prioritize, and assess suppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process |
| | | ID.SC-3: Require suppliers and third-party providers (by contractual requirement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan |
| | | ID.SC-4: Routinely assess suppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers |
| | | ID.SC-5: Conduct response and recovery planning and testing with suppliers and third-party providers |

(1) Asset Management. Each agency shall ensure that IT resources are identified and managed. Identification and management shall be consistent with the IT resource's relative importance to agency objectives and the organization's risk strategy. Specifically, each agency shall:

(a) Ensure that physical devices and systems within the organization are inventoried and managed (ID.AM-1).

(b) Ensure that software platforms and applications within the organization are inventoried and managed (ID.AM-2).

(c) Ensure that organizational communication and data flows are mapped and systems are designed or configured to regulate information flow based on data classification (ID.AM-3). Each agency shall:

1. Establish procedures that ensure only agency-owned or approved IT resources are connected to the agency internal network and resources.

2. Design and document its information security architecture using a defense-in-breadth approach. Design and documentation shall be assessed and updated periodically based on an agency-defined, risk-driven frequency that considers potential threat vectors (i.e., paths or tools that a threat actor may use to attack a target).

3. Consider diverse suppliers when designing the information security architecture.

(d) Each agency shall ensure that interdependent external information systems are catalogued (ID.AM-4). Agencies shall:

1. Verify or enforce required security controls on interconnected external IT resources in accordance with the information security policy or security plan.

2. Implement service level agreements for non-agency provided technology services to ensure appropriate security controls are established and maintained.

3. For non-interdependent external IT resources, execute information sharing or processing agreements with the entity receiving the shared information or hosting the external system in receipt of shared information.

4. Restrict or prohibit portable storage devices either by policy or a technology that enforces security controls for such devices.

5. Authorize and document inter-agency system connections.

6. Require that (e.g., contractually) external service providers adhere to agency security policies.

7. Document agency oversight expectations, and periodically monitor provider compliance.

(e) Each agency shall ensure that IT resources (hardware, data, personnel, devices and software) are categorized, prioritized, and documented based on their classification, criticality, and business value (ID.AM-5). Agencies shall:

1. Perform a criticality analysis for each categorized IT resource and document the findings of the analysis conducted.

2. Designate an authorizing official for each categorized IT resource and document the authorizing official's approval of the security categorization.

3. Create a contingency plan for each categorized IT resource. The contingency plan shall be based on resource classification and identify related cybersecurity roles and responsibilities.

4. Identify and maintain a reference list of exempt, and confidential and exempt agency information or software and the associated applicable state and federal statutes and rules.

(f) Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (ID.AM-6). Each agency is responsible for:

1. Informing workers that they are responsible for safeguarding their passwords and other authentication methods.

2. Informing workers that they shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

3. Informing workers that use, or oversee or manage workers that use, IT equipment that they shall report suspected unauthorized activity, in accordance with agency-established incident reporting procedures.

4. Informing users that they shall take precautions that are appropriate to protect IT resources in their possession from loss, theft, tampering, unauthorized access, and damage. Consideration will be given to the impact that may result if the IT resource is lost, and safety issues relevant to protections identified in this subsection.

5. Informing users of the extent that they will be held accountable for their activities.

6. Informing workers that they have no reasonable expectation of privacy with respect to agency-owned or agency-managed IT resources.

7. Ensuring that monitoring, network sniffing, and related security activities are only to be performed by workers who have been assigned security-related responsibilities either via their approved position descriptions or tasks assigned to them.

8. Appointing an Information Security Manager (ISM). Agency responsibilities related to the ISM include:

a. Notifying the Department of Management Services (DMS) of ISM appointments and reappointments.

b. Specifying ISM responsibilities in the ISM position description.

c. Establishing an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process, including the comprehensive risk assessment required by section 282.318, F.S.; a Computer Security Incident Response Team; and a disaster recovery program that aligns with the agency's Continuity of Operations (COOP) Plan.

d. Each agency ISM shall be responsible for the information security program plan.

9. Performing background checks and ensuring that a background investigation is performed on all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher. See paragraph 60GG-2.002(4)(a), F.A.C. These positions often, if not always, have privileged access. As such, in addition to agency-required background screening, background checks conducted by agencies shall include a federal criminal history check that screens for felony

convictions that concern or involve the following:

a. Computer related or IT crimes;

b. Identity theft crimes;

c. Financially-related crimes, such as: fraudulent practices, false pretenses and frauds, credit card crimes;

d. Forgery and counterfeiting;

e. Violations involving checks and drafts;

f. Misuse of medical or personnel records; and,

g. Theft.

Each agency shall establish appointment selection disqualifying criteria for individuals hired as IT workers that will have access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher.

(2) Business Environment. Each agency's cybersecurity roles, responsibilities, and IT risk management decisions shall align with the agency's mission, objectives, and activities. To accomplish this, agencies shall:

(a) Identify and communicate the agency's role in the business mission of the state (ID.BE-1).

(b) Identify and communicate the agency's place in critical infrastructure and its industry sector to inform internal stakeholders of IT strategy and direction (ID.BE-2).

(c) Establish and communicate priorities for agency mission, objectives, and activities (ID.BE-3).

(d) Identify system dependencies and critical functions for delivery of critical services (ID.BE-4).

(e) Implement information resilience requirements to support the delivery of critical services for all operating states (ID.BE-5).

(3) Governance. Each agency shall establish policies, procedures, and processes to manage and monitor the agency's operational IT requirements based on the agency's assessment of risk. Procedures shall address providing timely notification to management of cybersecurity risks. Agencies shall also:

(a) Establish and communicate a comprehensive cybersecurity policy (ID.GV-1).

(b) Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners (ID.GV-2).

(c) Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations (ID.GV-3).

(d) Ensure governance and risk management processes address cybersecurity risks (ID.GV-4).

(4) Risk Assessment.

(a) Approach. Each agency shall identify and manage the cybersecurity risk to agency operations (including mission, functions, image, or reputation), agency assets, and individuals using the following approach, that derives from the NIST Risk Management Framework (RMF) which may be found at: http://csrc.nist.gov/groups/SMA/fisma/framework.html. The Risk Assessment steps provided in the table below must be followed; however, agencies may identify and, based on the risk to be managed, consider other risk assessment security control requirements and frequency of activities necessary to manage the risk at issue.

| **Risk Assessments** | |
|---|---|
| Categorize: | Categorize information systems and the information processed, stored, and transmitted by that system based on a security impact analysis. |
| Select: | Select baseline security for information systems based on the security categorization; tailoring and supplementing the security baseline as needed based on organization assessment of risk and local conditions. |
| Implement: | Implement the selected baseline security and document how the controls are deployed within information systems and environment of operation. |
| Assess: | Assess the baseline security using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for systems. |
| Authorize: | Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the state resulting from the operation of the information system and the decision that this risk is acceptable. |
| Monitor: | Monitor and assess selected baseline security in information systems on an ongoing basis including assessing control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of systems to appropriate agency officials. |

Agencies are required to consider the following security objectives when assessing risk and determining what kind of assessment is required and when or how often an assessment is to occur: confidentiality, integrity and availability. When determining the potential impact to these security objectives agencies will use the following table, taken from the Federal Information Processing Standards (FIPS) Publication No. 199 (February 2004), which is hereby incorporated into this rule by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06498.

| **POTENTIAL IMPACT** | | | |
|---|---|---|---|
| Security Objectives: | LOW | MODERATE | HIGH |
| **Confidentiality** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability** Ensuring timely and reliable access to and use of information. | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

In accordance with section 282.318(4)(d), F.S., each agency shall complete and submit to DMS no later than July 31, 2017, and every three years thereafter, a comprehensive risk assessment. In completing the risk assessment agencies shall follow the six-step process ("Conducting the Risk Assessment") outlined in Section 3.2 of NIST Special Publication 800-30, utilizing the exemplary tables provided therein as applicable to address that particular agency's threat situation. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1 (September 2012) is hereby incorporated by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06499. When establishing risk management processes, it may be helpful for agencies to review NIST Risk Management Framework Special Publications – they can be downloaded from the following website: http://csrc.nist.gov/publications/PubsSPs.html. When assessing risk, agencies shall estimate the magnitude of harm resulting from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. Estimates shall be documented as low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

(b) Other agency risk management activities that agencies shall perform:

1. Identify and document asset vulnerabilities (ID.RA-1), business processes and protection requirements. Establish procedures to analyze systems and applications to ensure security controls are effective and appropriate.

2. Receive and manage cyber threat intelligence from information sharing forums and sources that contain information relevant to the risks or threats (ID.RA-2).

3. Identify and document internal and external threats (ID.RA-3).

4. Identify potential business impacts and likelihoods (ID.RA-4).

5. Use threats, vulnerabilities, likelihoods, and impacts to determine risk (ID.RA-5).

6. Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation (ID.RA-6).

(5) Risk Management. Each agency shall ensure that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Each agency shall:

(a) Establish risk management processes that are managed and agreed to by agency stakeholders and the agency head (ID.RM-1).

1. Establish a risk steering workgroup that ensures risk management processes are authorized by agency stakeholders. The risk steering workgroup must include a member of the agency IT unit and shall determine the appropriate meeting frequency and agency stakeholders.

(b) Identify and clearly document organizational risk tolerance based on the confidential and exempt nature of the data created, received, maintained, or transmitted by the agency; by the agency's role in critical infrastructure and sector specific analysis (ID.RM-2).

(c) Determine risk tolerance as necessary, based upon: analysis of sector specific risks; the agency's industry sector; agency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for agencies that maintain this information); and the agency's role in the state's mission (ID.RM-3).

(d) Establish parameters for IT staff participation in procurement activities.

(e) Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).

(f) Implement appropriate security controls for software applications obtained, purchased, leased, or developed to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other IT resources.

(g) Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment. Validate that IT resources conform to agency standard configurations prior to implementation into the production environment.

(6) Supply Chain Risk Management. Each agency shall establish priorities, constraints, risk tolerances, and assumptions to support risk decisions associated with managing supply chain risk. Each agency shall:

(a) Establish management processes to identify, establish, assess, and manage cyber supply chain risks which are agreed to by organizational stakeholders (ID.SC-1).

(b) Identify, prioritize, and assess suppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process (ID.SC-2).

(c) Require suppliers and third-party providers (by contractual agreement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan (ID.SC-3).

(d) Routinely assess suppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers (ID.SC-4).

(e) Conduct response and recovery planning and testing with suppliers and third-party providers (ID.SC-5).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-16-16, Amended 2-5-19, Formerly 74-2.002.*

**60GG-2.003 Protect.**

The protect function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Protect (PR) | Identity Management, Authentication, | PR.AC-1: Issue, manage, verify, revoke, and audit identities and credentials for authorized devices, processes, and users |
| | | PR.AC-2: Manage and protect physical access to assets |

| | |
|---|---|
| and Access Control (AC) | PR.AC-3: Manage remote access |
| | PR.AC-4: Manage access permissions and authorizations, incorporate the principles of least privilege and separation of duties |
| | PR.AC-5: Protect network integrity, by incorporating network segregation and segmentation where appropriate |
| | PR.AC-6: Proof and bond identities to credentials, asserting in interactions when appropriate (see token control definition) |
| | PR.AC-7: Authenticate credentials assigned to users, devices, and other assets commensurate with the risk of the transaction. |
| Awareness and Training (AT) | PR.AT-1: Inform and train all users |
| | PR.AT-2: Ensure that privileged users understand roles and responsibilities |
| | PR.AT-3: Ensure that third-party stakeholders understand roles and responsibilities |
| | PR.AT-4: Ensure that senior executives understand roles and responsibilities |
| | PR.AT-5: Ensure that physical and cybersecurity personnel understand their roles and responsibilities |
| Data Security (DS) | PR.DS-1: Protect data-at-rest |
| | PR.DS-2: Protect data-in-transit |
| | PR.DS-3: Formally manage assets managed throughout removal, transfers, and disposition |
| | PR.DS-4: Ensure that adequate capacity is maintained to support availability needs |
| | PR.DS-5: Implement data leak protection measures |
| | PR.DS-6: Use integrity checking mechanisms to verify software, firmware, and information integrity |
| | PR.DS-7: Logically or physically separate the development and testing environment(s) from the production environment |
| | PR.DS-8: Use integrity checking mechanisms to verify hardware integrity |
| Information Protection Processes and Procedures | PR.IP-1: Create and maintain a baseline configuration that incorporates all security principles for information technology/industrial control systems |
| | PR.IP-2: Implement a System Development Life Cycle (SDLC) to manage systems |
| | PR.IP-3: Establish configuration change control processes |
| | PR.IP-4: Conduct, maintain, and test backups of information |
| | PR.IP-5: Meet policy and regulatory requirements that are relevant to the physical operating environment for organizational assets |
| | PR.IP-6: Destroy data according to policy |
| | PR.IP-7: Continuously improve protection processes |
| | PR.IP-8: Share effectiveness of protection technologies with stakeholders that should or must receive this information |
| | PR.IP-9: Establish and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) |
| | PR.IP-10: Test response and recovery plans |
| | PR.IP-11: Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening) |
| | PR.IP-12: Develop and implement a vulnerability management plan |
| Maintenance (MA) | PR.MA-1: Perform and log maintenance and repair of organizational assets, with approved and controlled tools |
| | PR.MA-2: Approve, log, and perform remote maintenance of agency assets in a manner that prevents unauthorized access |
| Protective Technology | PR.PT-1: Determine, document, implement, and review audit/log records in accordance with policy |

| | | |
|---|---|---|
| | (PT) | PR.PT-2: Protect and restrict removable media usage according to policy |
| | | PR.PT-3: Incorporate the principle of least functionality by configuring systems to provide only essential capabilities |
| | | PR.PT-4: Protect communications and control networks |
| | | PR.PT-5: Implement mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations |

(1) Access Control. Each agency shall ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Specifically:

(a) Each agency shall manage identities and credentials for authorized devices and users (PR.AC-1). Control measures shall, at a minimum include authentication token(s) unique to the individual.

Agencies shall:

1. Require that all agency-owned or approved computing devices, including mobile devices, use unique user authentication.

2. Require users to log off or lock their workstations prior to leaving the work area.

3. Require inactivity timeouts that log-off or lock workstations or sessions.

4. Locked workstations or sessions must be locked in a way that requires user authentication with an authentication token(s) unique to the individual user to disengage.

5. When passwords are used as the sole authentication token, require users to use complex passwords that are changed at least every 90 days.

6. Address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations and facilitate periodic review of access rights with information owners. Frequency of reviews shall be based on system categorization or assessed risk.

7. Establish access disablement and notification timeframes for worker separations. The agency will identify the appropriate person in the IT unit to receive notification. Notification timeframes shall consider risks associated with system access post-separation.

8. Ensure IT access is removed when the IT resource is no longer required.

9. Require MFA for access to networks or applications that have a categorization of moderate, high, or contain exempt, or confidential and exempt, information. This excludes externally hosted systems designed to deliver services to agency customers where the agency documents the analysis and the risk steering workgroup accepts the associated risk.

10. Require MFA for access to privileged accounts.

(b) Each agency shall manage and protect physical access to assets (PR.AC-2). In doing so, agency security procedures or controls shall:

1. Address protection of IT resources from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturer specifications.

2. Implement procedures to manage physical access to IT facilities and/or equipment.

3. Identify physical controls that are appropriate for the size and criticality of the IT resources.

4. Specify physical access to information resource facilities and/or equipment that is restricted to authorized personnel.

5. Detail visitor access protocols, including recordation procedures, and in locations housing systems categorized as moderate-impact or high-impact, require that visitors be supervised by authorized personnel.

6. Address how the agency will protect network integrity by incorporating network segregation.

(c) Each agency shall manage remote access (PR.AC-3). In doing so, agencies shall:

1. Address how the agency will securely manage and document remote access.

2. Specify that only secure, agency-managed, remote access methods may be used to remotely connect computing devices to the agency internal network.

3. For systems containing exempt, or confidential and exempt data, ensure written agreements and procedures are in place to ensure security for sharing, handling or storing confidential data with entities outside the agency.

(d) Each agency shall ensure that access permissions and authorizations, are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4). In doing so, agencies shall:

1. Execute interconnection security agreements to authorize, document, and support continual management of inter-agency connected systems.

2. Manage access permissions by incorporating the principles of “least privilege” and “separation of duties.”

3. Specify that all workers be granted access to agency IT resources based on the principles of “least privilege” and “need to know determination.”

4. Specify that system administrators restrict and tightly control the use of system development utility programs that may be capable of overriding system and application controls.

(e) Each agency shall ensure that network integrity is protected, incorporating network segregation and segmentation where appropriate (PR.AC-5).

(f) Proof and bond identities to credentials and assert in interactions when appropriate (PR.AC-6).

(g) Authenticate users, devices, and other assets commensurate with the risk of the transaction (PR.AC-7).

(2) Awareness and Training. Agencies shall provide all their workers cybersecurity awareness education and training so as to ensure they perform their cybersecurity related duties and responsibilities consistent with agency policies and procedures. In doing so, each agency shall:

(a) Inform and train all workers (PR.AT-1).

(b) Ensure that privileged users understand their roles and responsibilities (PR.AT-2).

(c) Ensure that third-party stakeholders understand their roles and responsibilities (PR.AT-3).

(d) Ensure that senior executives understand their roles and responsibilities (PR.AT-4).

(e) Ensure that physical and cybersecurity personnel understand their roles and responsibilities (PR.AT-5).

(3) For each of the above subsections the following shall also be addressed:

(a) Appoint a worker to coordinate the agency information security awareness program. If an IT security worker does not coordinate the security awareness program, they shall be consulted for content development purposes. Agencies will ensure that all workers (including volunteer workers) are clearly notified of applicable obligations, established via agency policies, to maintain compliance with such controls.

(b) Establish a program that includes, at a minimum, annual security awareness training and on-going education and reinforcement of security practices.

(c) Provide training to workers within 30 days of start date.

(d) Include security policy adherence expectations for the following, at a minimum: disciplinary procedures and implications, acceptable use restrictions, data handling (procedures for handling exempt and confidential and exempt information), telework and cybersecurity incident reporting procedures. Incident reporting procedures shall:

1. Establish requirements for workers to immediately report loss of mobile devices, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency reporting procedures.

(e) Where technology permits, provide training prior to system access. For specialized agency workers (e.g., law enforcement officers) who are required to receive extended off-site training prior to reporting to their permanent duty stations, initial security awareness training shall be provided within 30 days of the date they report to their permanent duty station.

(f) Require, prior to access, workers verify in writing that they will comply with agency IT security policies and procedures.

(g) Document parameters that govern personal use of agency IT resources and define what constitutes personal use. Personal use, if allowed by the agency, shall not interfere with the normal performance of any worker’s duties, or consume significant or unreasonable amounts of state IT resources (e.g., bandwidth, storage).

(h) Inform workers of what constitutes inappropriate use of IT resources. Inappropriate use shall include, but may not be limited to, the following:

1. Distribution of malware.

2. Disablement or circumvention of security controls.

3. Forging headers.

4. Political campaigning or unauthorized fundraising.

5. Use for personal profit, benefit or gain.

6. Offensive, indecent, or obscene access or activities, unless required by job duties.

7. Harassing, threatening, or abusive activity.

8. Any activity that leads to performance degradation.

9. Auto-forwarding to external email addresses.

10. Unauthorized, non-work-related access to: chat rooms, political groups, singles clubs or dating services; peer-to-peer file

sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker web-site/software; and pornography and sites containing obscene materials.

(4) Data Security. Each agency shall manage and protect records and data, including data-at-rest, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Agencies shall establish procedures, and develop and maintain agency cryptographic implementations. Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, and prevention of unauthorized substitution. Also, key management processes must be in place and verified prior to encrypting data at rest, to prevent data loss and support availability. In protecting data security, agencies shall:

(a) Protect data-at-rest by establishing (PR.DS-1):

1. Procedures that ensure only agency-owned or approved IT resources are used to store confidential or exempt information.

2. Procedures that ensure agency-owned or approved portable IT resources containing confidential or mission critical data are encrypted.

3. Procedures that ensure agency-owned or approved portable IT resources that connect to the agency internal network use agency-managed security software.

4. Inform users not to store unique copies of agency data on workstations or mobile devices.

(b) Protect data-in-transit (PR.DS-2). Each agency shall:

1. Encrypt confidential and exempt information during transmission, except when the transport medium is owned or managed by the agency and controls are in place to protect the data during transit.

2. Ensure that wireless transmissions of agency data employ cryptography for authentication and transmission.

3. Make passwords unreadable during transmission and storage.

4. Encrypt mobile IT resources that store, process, or transmit exempt, or confidential and exempt agency data.

(c) Formally manage assets throughout removal, transfer, and disposition (PR.DS-3).

1. Ensure any records stored on storage media to be disposed of or released for reuse, are sanitized or destroyed in accordance with organization-developed procedures and the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.

2. Destruction of confidential or exempt information shall be conducted such that the information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.

3. Document procedures for sanitization of agency-owned IT resources prior to reassignment or disposal.

4. Equipment sanitization shall be performed such that confidential or exempt information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction. File deletion and media formatting are not acceptable methods of sanitization. Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

(d) Maintain adequate capacity to ensure system availability and data integrity (PR.DS-4).

1. Ensure adequate audit/log capacity.

2. Protect against or limit the effects of denial of service attacks.

(e) Implement protections against data leaks or unauthorized data disclosures by establishing policies and procedures that address (PR.DS-5):

1. Appropriate handling and protection of exempt, and confidential and exempt, information. Policies shall be reviewed and acknowledged by all workers.

2. Retention and destruction of confidential and exempt information in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.

3. Access agreements for agency information systems.

4. Boundary protection.

5. Transmission confidentiality and integrity.

(f) Employ integrity checking mechanisms to verify software, firmware, and information integrity (PR.DS-6).

1. Application controls shall be established to ensure the accuracy and completeness of data, including validation and integrity checks, to detect data corruption that may occur through processing errors or deliberate actions.

(g) Physically or logically separate development and testing environment(s) from the production environment and ensure that

production exempt, or confidential and exempt data is not used for development where technology permits. Production exempt, or confidential and exempt data may be used for testing if the data owner authorizes the use and regulatory prohibitions do not exist; the test environment limits access and access is audited; and production exempt, and confidential and exempt data is removed from the system when testing is completed. Data owner authorization shall be managed via technical means, to the extent practical (PR.DS-7).

(h) Use integrity checking mechanisms to verify hardware integrity (PR.DS-8). In doing so, agencies shall establish processes to protect against and/or detect unauthorized changes to hardware used to support systems with a categorization of high-impact.

(5) Information Protection Processes and Procedures. Each agency shall ensure that security policies, processes and procedures are maintained and used to manage protection of information systems and assets. Such policies, processes and procedures shall:

(a) Include a current baseline configuration of information systems which incorporate security principles (PR.IP-1). Baselines shall:

1. Specify standard hardware and secure standard configurations.

2. Include documented firewall and router configuration standards, and include a current network diagram.

3. Require that vendor default settings, posing security risks, are changed or disabled for agency-owned or managed IT resources, including encryption keys, accounts, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure device security settings are enabled where appropriate.

4. Allow only agency-approved software to be installed on agency-owned IT resources.

(b) Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2). In doing so, agencies shall:

1. Develop and implement processes that include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

2. Ensure security reviews are approved by the ISM and Chief Information Officer (or designee) before new or modified applications or technologies are moved into production. For IT resources housed in a state data center, the security review shall also be approved by the data center before the new or modified applications or technologies are moved into production.

3. The application development team at each agency shall implement appropriate security controls to minimize risks to agency IT resources and meet the security requirements of the application owner. Agencies will identify in their policies, processes and procedures the security coding guidelines the agency will follow when obtaining, purchasing, leasing or developing software.

4. Where technology permits, the agency shall ensure anti-malware software is maintained on agency IT resources.

(c) Establish a configuration change control process to manage upgrades and modifications to existing IT resources (PR.IP-3). In doing so, agencies shall:

1. Determine types of changes that are configuration-controlled (e.g. emergency patches, releases, and other out-of-band security packages).

2. Develop a process to review and approve or disapprove proposed changes based on a security impact analysis (e.g., implementation is commensurate with the risk associated with the weakness or vulnerability).

3. Develop a process to document change decisions.

4. Develop a process to implement approved changes and review implemented changes.

5. Develop an oversight capability for change control activities.

6. Develop procedures to ensure security requirements are incorporated into the change control process.

(d) Ensure backups of information are conducted, maintained, and tested (PR.IP-4).

(e) Establish policy and regulatory expectations for protection of the physical operating environment for agency-owned or managed IT resources (PR.IP-5).

(f) Manage and dispose of records/data in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies (PR.IP-6).

(g) Establish a policy and procedure review process that facilitates continuous improvement to protection processes (PR.IP-7). Each agency shall:

1. Ensure system security control selection occurs during the beginning of the SDLC and is documented in final design documentation.

2. Ensure system security plans shall document controls necessary to protect production data in the production environment and copies of production data used in non-production environments.

3. Ensure system security plans are confidential per section 282.318, F.S., and shall be available to the agency ISM.

4. Require that each agency application or system with a categorization of moderate-impact or higher have a documented system security plan (SSP). For existing production systems that lack a SSP, a risk assessment shall be performed to determine prioritization of subsequent documentation efforts. The SSP shall include provisions that:

(I) Align the system with the agency's enterprise architecture.

(II) Define the authorization boundary for the system.

(III) Describe the mission-related business purpose.

(IV) Provide the security categorization, including security requirements and rationale (compliance, availability, etc.).

(V) Describe the operational environment, including relationships, interfaces, or dependencies on external services.

(VI) Provide an overview of system security requirements.

(VII) Identify authorizing official or designee, who reviews and approves prior to implementation.

5. Require information system owners (ISOs) to define application security-related business requirements using role-based access controls and rule-based security policies where technology permits.

6. Require ISOs to establish and authorize the types of privileges and access rights appropriate to system users, both internal and external.

7. Create procedures to address inspection of content stored, processed or transmitted on agency-owned or managed IT resources, including attached removable media. Inspection shall be performed where authorization has been provided by stakeholders that should or must receive this information.

8. Establish parameters for agency-managed devices that prohibit installation (without worker consent) of clients that allow the agency to inspect private partitions or personal data.

9. Require ISOs ensure segregation of duties when establishing system authorizations.

10. Establish controls that prohibit a single individual from having the ability to complete all steps in a transaction or control all stages of a critical process.

11. Require agency information owners to identify exempt, and confidential and exempt information in their systems.

(h) Ensure that effectiveness of protection technologies is shared with stakeholders that should or must receive this information (PR.IP-8).

(i) Develop, implement and manage response plans (e.g., Incident Response and Business Continuity) and recovery plans (e.g., Incident Recovery and Disaster Recovery) (PR.IP-9).

(j) Establish a procedure that ensures that agency response and recovery plans are regularly tested (PR.IP-10).

(k) Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening) (PR.IP-11).

(l) Each agency shall develop and implement a vulnerability management plan (PR.IP-12).

(6) Maintenance. Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures. Each agency shall:

(a) Perform and log maintenance and repair of IT resources, with tools that have been approved and are administered by the agency to be used for such activities (PR.MA-1).

(b) Approve, encrypt, log and perform remote maintenance of IT resources in a manner that prevents unauthorized access (PR.MA-2).

(c) Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing agency-developed authenticators in legacy applications.

(7) Protective Technology. Each agency shall ensure that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Specifically, each agency shall:

(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with agency-developed policy. Agency-developed policy shall be based on resource criticality. Where possible, ensure that electronic audit records allow actions of users to be uniquely traced to those users so they can be held accountable for their actions. Maintain logs identifying where access to exempt, or confidential and exempt data was permitted. The logs shall support unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed or transmitted by the individual (PR.PT-1).

(b) Protect and restrict removable media in accordance with agency-developed information security policy (PR.PT-2).

(c) Incorporate the principle of least functionality by configuring systems to only provide essential capabilities (PR.PT-3).

(d) Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources (PR.PT-4). Agencies shall:

1. Place databases containing mission critical, exempt, or confidential and exempt data in an internal network zone, segregated from the demilitarized zone (DMZ).

2. Agencies shall require host-based (e.g., a system controlled by a central or main computer) boundary protection on mobile computing devices where technology permits (i.e., detection agent).

(e) Implement mechanisms (e.g., failsafe, load balancing across duplicated systems, hot swap) to achieve resilience requirements in normal and adverse situations (PR.PT-5).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.003.*

**60GG-2.004 Detect.**

The detect function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Detect (DE) | Anomalies and Events (AE) | DE.AE-1: Establish and manage a baseline of network operations and expected data flows for users and systems |
| | | DE.AE-2: Analyze detected cybersecurity events to understand attack targets and methods |
| | | DE.AE-3: Collect and correlate cybersecurity event data from multiple sources and sensors |
| | | DE.AE-4: Determine the impact of cybersecurity events |
| | | DE.AE-5: Establish incident alert thresholds |
| | Security Continuous Monitoring (CM) | DE.CM-1: Monitor the network to detect potential cybersecurity events |
| | | DE.CM-2: Monitor the physical environment to detect potential cybersecurity events |
| | | DE.CM-3: Monitor personnel activity to detect potential cybersecurity events |
| | | DE.CM-4: Detect malicious code |
| | | DE.CM-5: Detect unauthorized mobile code |
| | | DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events |
| | | DE.CM-7: Monitor for unauthorized personnel, connections, devices, and software |
| | | DE.CM-8: Perform vulnerability scans |
| | Detection Processes (DP) | DE.DP-1: Define roles and responsibilities for detection to ensure accountability |
| | | DE.DP-2: Ensure that detection activities comply with all applicable requirements |
| | | DE.DP-3: Test detection processes |
| | | DE.DP-4: Communicate event detection information to stakeholders that should or must receive this information |
| | | DE.DP-5: Continuously improve detection processes |

(1) Anomalies and Events. Each agency shall develop policies and procedures that will facilitate detection of anomalous activity and that allow the agency to understand the potential impact of events.

Such policies and procedures shall:

(a) Establish and manage a baseline of network operations and expected data flows for users and systems (DE.AE-1).

(b) Detect and analyze anomalous cybersecurity events to determine attack targets and methods (DE.AE-2).

1. Monitor for unauthorized wireless access points connected to the agency internal network, and immediately remove them upon detection.

2. Implement procedures to establish accountability for accessing and modifying exempt, or confidential and exempt, data stores to ensure inappropriate access or modification is detectable.

(c) Collect and correlate cybersecurity event data from multiple sources and sensors (DE.AE-3).

(d) Determine the impact of cybersecurity events (DE.AE-4).

(e) Establish incident alert thresholds (DE.AE-5).

(2) Security Continuous Monitoring. Each agency shall determine the appropriate level of monitoring that will occur regarding IT resources necessary to identify cybersecurity events and verify the effectiveness of protective measures. Such activities shall

include:

(a) Monitoring the network to detect potential cybersecurity events (DE.CM-1).

(b) Monitoring for unauthorized IT resource connections to the internal agency network.

(c) Monitoring the physical environment to detect potential cybersecurity events (DE.CM-2).

(d) Monitoring user activity to detect potential cybersecurity events (DE.CM-3).

(e) Monitoring for malicious code (DE.CM-4).

(f) Monitoring for unauthorized mobile code (DE.CM-5).

(g) Monitoring external service provider activity to detect potential cybersecurity events (DE.CM-6).

(h) Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7).

(i) Performing vulnerability scans (DE.CM-8). These shall be a part of the System Development Life Cycle (SDLC).

(3) Detection Processes. Each agency shall maintain and test detection processes and procedures to ensure awareness of anomalous events. These procedures shall be based on assigned risk and include the following:

(a) Defining roles and responsibilities for detection to ensure accountability (DE.DP-1).

(b) Ensuring that detection activities comply with all applicable requirements (DE.DP-2).

(c) Testing detection processes (DE.DP-3).

(d) Communicating event detection information to stakeholders that should or must receive this information (DE.DP-4).

(e) Continuously improving detection processes (DE.DP-5).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.004.*

**60GG-2.005 Respond.**

The respond function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Respond (RS) | Response Planning (RP) | RS.RP-1: Execute response plan during or after an incident |
| | Communications (CO) | RS.CO-1: Ensure that personnel know their roles and order of operations when a response is needed |
| | | RS.CO-2: Report incidents consistent with established criteria |
| | | RS.CO-3: Share information consistent with response plans |
| | | RS.CO-4: Coordinate with stakeholders consistent with response plans |
| | | RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness |
| | Analysis (AN) | RS.AN-1: Investigate notifications from detection systems |
| | | RS.AN-2: Understand the impact of incidents |
| | | RS.AN-3: Perform forensic analysis |
| | | RS.AN-4: Categorize incidents consistent with response plans |
| | | RS.AN-5: Establish processes to receive, analyze, and respond to vulnerabilities disclosed to the agency from internal and external sources |
| | Mitigation (MI) | RS.MI-1: Contain incidents |
| | | RS.MI-2: Mitigate incidents |
| | | RS.MI-3: Mitigate newly identified vulnerabilities or document accepted risks |
| | Improvements (IM) | RS.IM-1: Incorporate lessons learned in response plans |
| | | RS.IM-2: Periodically update response strategies |

(1) Response Planning. Each agency shall establish and maintain response processes and procedures and validate execution capability to ensure agency response for detected cybersecurity incidents. Each agency shall execute a response plan during or after an incident (RS.RP-1).

(a) Agencies shall establish a Computer Security Incident Response Team (CSIRT) to respond to cybersecurity incidents. CSIRT members shall convene immediately, upon notice of cybersecurity incidents. Responsibilities of CSIRT members include:

1. Convening a simple majority of CSIRT members at least quarterly to review, at a minimum, established processes and

escalation protocols.

2. Receiving incident response training annually. Training shall be coordinated as a part of the information security program.

3. CSIRT membership shall include, at a minimum, a member from the information security team, the CIO (or designee), and a member from the Inspector General's Office who shall act in an advisory capacity. The CSIRT team shall report findings to agency management.

4. The CSIRT shall determine the appropriate response required for each cybersecurity incident.

5. The agency security incident reporting process must include notification procedures, established pursuant to section 501.171, F.S., section 282.318, F.S., and as specified in executed agreements with external parties. For reporting incidents to DMS and the Cybercrime Office (as established within the Florida Department of Law Enforcement via section 943.0415, F.S.), agencies shall report observed incident indicators via the DMS Incident Reporting Portal to provide early warning and proactive response capability to other State of Florida agencies. Such indicators may include any known attacker IP addresses, malicious uniform resource locator (URL) addresses, malicious code file names and/or associated file hash values.

(2) Communications. Each agency shall coordinate response activities with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. Each agency shall:

(a) Inform workers of their roles and order of operations when a response is needed (RS.CO-1).

(b) Require that incidents be reported consistent with established criteria and in accordance with agency incident reporting procedures. Criteria shall require immediate reporting, including instances of lost identification and authentication resources (RS.CO-2).

(c) Share information, consistent with response plans (RS.CO-3).

(d) Coordinate with stakeholders, consistent with response plans (RS.CO-4).

(e) Establish communications with external stakeholders to share and receive information to achieve broader cybersecurity situational awareness (RS.CO-5). Where technology permits, enable automated security alerts. Establish processes to receive, assess, and act upon security advisories.

(3) Analysis. Each agency shall conduct analysis to adequately respond and support recovery activities. Related activities include:

(a) Each agency shall establish notification thresholds and investigate notifications from detection systems (RS.AN-1).

(b) Each agency shall assess and identify the impact of incidents (RS.AN-2).

(c) Each agency shall perform forensics, where deemed appropriate (RS.AN-3).

(d) Each agency shall categorize incidents, consistent with response plans (RS.AN-4). Each incident report and analysis, including findings and corrective actions, shall be documented.

(e) Establish processes to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (RS.AN-5).

(4) Mitigation. Each agency shall perform incident mitigation activities. The objective of incident mitigation activities shall be to: attempt to contain and prevent recurrence of incidents (RS.MI-1); mitigate incident effects and resolve the incident (RS.MI-2); and address vulnerabilities or document as accepted risks.

(5) Improvements. Each agency shall improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into response plans (RS.IM-1). Agencies shall update response strategies in accordance with agency-established policy (RS.IM-2).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.005.*

**60GG-2.006 Recover.**

The recover function of the FCS is visually represented as such:

| Function | Category | Subcategory |
|---|---|---|
| Recover (RC) | Recovery Planning (RP) | RC.RP-1: Execute recovery plan during or after a cybersecurity incident |
| | Improvements (IM) | RC.IM-1: Incorporate lessons learned in recovery plans |
| | | RC.IM-2: Periodically update recovery strategies |
| | Communications (CO) | RC.CO-1: Manage public relations |
| | | RC.CO-2: Repair reputation after an event |

| | | |
|---|---|---|
| | | RC.CO-3: Communicate recovery activities to internal stakeholders and executive and management teams |

(1) Recovery Planning. Each agency shall execute and maintain recovery processes and procedures to ensure restoration of systems or assets affected by cybersecurity incidents. Each agency shall:

(a) Execute a recovery plan during or after an incident (RC.RP-1).

(b) Mirror data and software, essential to the continued operation of critical agency functions, to an off-site location or regularly back up a current copy and store at an off-site location.

(c) Develop procedures to prevent loss of data, and ensure that agency data, including unique copies, are backed up.

(d) Document disaster recovery plans that address protection of critical IT resources and provide for the continuation of critical agency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical agency functions.

(e) IT disaster recovery plans shall be tested at least annually; results of the annual exercise shall document plan procedures that were successful and specify any modifications required to improve the plan.

(2) Improvements. Each agency shall improve recovery planning and processes by incorporating lessons learned into future activities. Such activities shall include:

(a) Incorporating lessons learned in recovery plans (RC.IM-1).

(b) Updating recovery strategies (RC.IM-2).

(3) Communications. Each agency shall coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Such activities shall include:

(a) Managing public relations (RC.CO-1).

(b) Attempts to repair reputation after an event, if applicable (RC.CO-2).

(c) Communicating recovery activities to stakeholders, internal and external where appropriate (RC.CO-3).

*Rulemaking Authority 282.318(6) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.006.*