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(19), 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(28), 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(18), F.S.

4. Threat – see Section 282.0041(36), F.S.

Rulemaking Authority 282.318(11) 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(11) 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(11) 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(11) 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(11) 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(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.006.