UNIVERSITY OF THE DISTRICT OF COLUMBIA
1851

INFORMATION SECURITY INCIDENT RESPONSE POLICY

1. **Purpose**

   This policy aims to ensure that the University is prepared to respond to information security incidents, protect University Information Systems, and prevent disruption of University Information Resources by providing the required management for incident handling, reporting, and monitoring.

2. **Scope and Applicability**

   This policy and its supporting standards and procedures apply to all Users who use or have access to UDC Information Systems and Information Resources.

3. **Definitions**

   Capitalized terms shall have the meaning ascribed to them herein and shall have the same meaning when used in the singular or plural form or any appropriate tense.

   1. **Availability:** The principle of ensuring timely and reliable access to and use of Information based upon the concept of Least Privilege.

   2. **Confidentiality:** The principle of preserving authorized restrictions on Information access and disclosure, including means for protecting personal privacy and proprietary information.

   3. **Computer Incident Response Team (CIRT):** A group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents.

   4. **Contractor:** A person or company undertaking a contract to provide materials or labor to perform a service.

5. **Data:** Data is element(s) of Information in the form of facts, such as numbers, words, names, or descriptions of things from which "understandable information" can be derived.

6. **Employee:** University staff and faculty, including nonexempt, exempt, and overseas staff and collegiate faculty.

7. **High Risk:** Any Security Incident with (i) a significant impact on University Information Systems, Information Resources, or operations, (ii) the potential for significant negative financial or public relations impact, or (iii) a legal impact on the University.

8. **Information:** Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numeric, graphic, cartographic, narrative, or audiovisual.

9. **Information Resource:** Anything that is intended to generate, store, or transmit Information.

10. **Information Security:** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

11. **Information System Steward:** A UDC staff member or other individual providing services to the University who is responsible for the development, procurement, compliance, and/or final disposition of an Information System.

12. **Information System:** Inter-related components of Information Resources working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

13. **Integrity:** Ensuring Records and the Information contained therein are accurate and Authentic by guarding against improper modification or destruction.

14. **Moderate Risk:** Any Security Incident with (i) moderate impact on the University Information Systems, Information Resources or operations and/or (ii) some limited risk of negative financial or public relations impact.

15. **Privacy:** The right of a party to maintain control over and Confidentiality of Information about itself.

16. **Security:** A condition resulting from establishing and maintaining protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

17. **Security Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies, including but not limited to, attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

18. **University:** University of the District of Columbia or UDC

19. **User:** A member of the University community, including but not limited to Staff and Faculty, and other individuals performing services on behalf of University, including Contractors, volunteers and other individuals who may have a need to access, use or control University Data.

4. Security Incident Response

1. Under the direction of the Information System Security Officer, a Computer Incident Response Team (CIRT) shall be established to ensure an appropriate response to Security Incidents. The CIRT shall consist of Employees and Contractors with the technical, administrative, and communication skills required to facilitate a prompt and thorough mitigation and remediation response to Security Incidents.

2. An information security incident response plan shall be developed and implemented that:

    1. Provides a well-defined, organized approach for responding to critical Security Incidents affecting University Information Resources and Information Systems.

    2. Describes the structure, roles, and responsibilities of the incident response capability

    3. Identifies management and key personnel and ensures they are notified of information Security Incidents as required

    4. Defines reportable incidents

    5. Defines Severity Classifications for Information Security Incidents (High, Moderate, Low)

3. Upon notification of a Security Incident, the Information System Security Officer (or designee) will conduct an initial investigation and decide whether to activate the CIRT.

4. The information security incident response plan and procedures shall be reviewed at least annually to address system/organizational changes or problems encountered during implementation, execution, or testing.

    5. Handling of all Information Security Incidents shall be documented in the Incident ticket, and all technology-specific remediation processes shall be documented in a procedures document.

    6. All operational units and other related University Employees and Contractors are required to provide the CIRT with any assistance requested for purposes of investigation, remediation, and reporting of an incident.

    7. Continuous monitoring must be deployed and be prepared to provide operational visibility and managed change control in support of Incident response duties.

5. **Incident Reporting**

    1. Any User who suspects or becomes aware of an Information Security Incident involving University information, Information Resources or Information Systems should contact the UDC technical support service desk as soon as possible by calling 1-202-274-5941, emailing support@udc.edu or contacting the UDC Chief Information Officer at suresh.murugan@udc.edu.

6. **Exceptions**

   Exceptions to this policy must be submitted to UDC Chief Information Officer at suresh.murugan@udc.edu for review and approval.

7. **Enforcement**

    1. Any Faculty, Staff, Contractor, or third-party performing duties on behalf of the University with knowledge of an alleged violation of this policy shall notify the Information System Security Officer as soon as practicable.

    2. Information System Stewards in consultation with the Office of Human Resources may instruct Access Account Managers, or other appropriate personnel to confiscate, temporarily suspend, or terminate Users' access to Information Resources while investigating an alleged violation of this policy.

    3. Any Employee, Contractor, or other third-party performing duties on behalf of the University who violates this policy may be denied access to Information Resources and may be subject to disciplinary action, up to and including termination of employment or contract.

8. **Effective Date:** This policy is effective as of the Version Effective Date set forth above and supersedes all prior policies on the subject matter hereof.