DUQUESNE UNIVERSITY
Computing and Technology Services

| Information Security Service Requirements | Effective Date: 7/1/2018<br>Responsible Officer: Charles Bartel, Vice President for Information Technology and Chief Information Officer |
|---|---|

1. **Purpose:**

The Information Security Service Requirement defines and describes the responsibilities and required practices for all members of the community with respect to information security and the protection of University data and information. This service requirement applies to all faculty, staff, students, third-party agents and other University affiliates who utilize Duquesne University information, data, and computing environments.

Duquesne University relies on a wide range of computing environments to meet its educational, community engagement, financial and operational requirements. It is therefore imperative that computer data, hardware, networks, and software be adequately protected and safeguarded against alteration, damage, theft, or unauthorized access & use.

2. **Organizational and Functional Responsibilities:**

a. **University Community Members.** It is the responsibility of University Community Members to:
   I. Protect University information and resources, including passwords,
   II. Report suspected information/computer security incidents to one or more of the following: the information owner, CTS Help Desk, the Director for Information Security and Chief Information Security Officer or General Counsel.
   III. Follow all university policies and CTS service requirements. Individuals can find a list of the IT related policies and service requirements at http://duq.edu/about/campus/computing-and-technology/policies.

b. **Vice President for Information Technology and Chief Information Officer (VP for IT & CIO).** The VP for IT & CIO has overall responsibility ensuring the implementation, enhancement, monitoring and enforcement of the Information Security Program.

   I. VP for IT & CIO will ensure that the organizational structure is in place for:
      i. Coordinating and implementing information security policies, standards and procedures;
      ii. assigning information security responsibilities;
      iii. implementing an information security awareness program;
      iv. responding to IT security incidents;
      v. leading major initiatives to enhance IT security;
      vi. monitor significant changes in the exposure of information assets to major threats, legal or regulatory requirements.

c. **Director for Information Security and Chief Information Security Officer (CISO).** The Director for Information Security & CISO, under the direction of the VP for IT & CIO, is responsible developing and managing a comprehensive cyber-security program the provides:
   I. a University-wide information security polices, standards and procedures;
   II. an information security awareness program; monitoring significant changes in the exposure of information assets to major threats;
   III. response plan for IT security incidents;
   IV. investigations of all alleged information security violations;
   V. development and implementation of major initiatives to enhance information security at Duquesne University.

d. **Information Technology (IT) Support Staff**. IT support staff have responsibility for managing the information data and computing environments at Duquesne University. It is their responsibility to support the Information Security Program and provide resources needed to enhance and maintain a level of information security consistent with industry best practices to protect the University. These individuals and organization have the following responsibilities to ensure information security environment at Duquesne University:
   I. Develop, maintain and enforce information security processes, policies and requirements.
   II. Oversee and validate that the proper security controls are implemented for which the University has assigned ownership responsibility, based on the University's classification designations.
   III. Validate that appropriate information security requirements for user access to automated information are defined for files, databases, and physical devices assigned within various areas of responsibility at the University.
   IV. Confirm that critical data and recovery plans are backed up and the associated recovery plans are developed jointly with data owners.

**3. Information Security Service Requirements:**

   I. All stored and transmitted electronic information regardless of form or format is an asset and must be protected from its creation, through its useful life, and to its authorized disposal. It must be maintained in a secure, accurate and reliable manner and be readily available for authorized use. Information must be classified and protected per the CTS Data Governance Service Requirements (http://duq.edu/about/campus/computing-and-technology/policies).
   II. Information is one of the University's most valuable assets and the University relies upon that information to support our mission. The quality and availability of that information is central to the University's ability to carry out its mission. Therefore, the security of the University's information, and of the technologies and systems that support it, is the responsibility of everyone concerned. Each authorized user of University information has an obligation to preserve and protect University information assets in a consistent and reliable manner. Information security controls provide the necessary physical, logical and procedural safeguards to accomplish those goals.
   III. **Confidentiality / Integrity / Availability:** All University information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. Information owners will secure information within their

jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.

IV. **Individual Accountability:** Individual accountability is the cornerstone of any information security program. Without it, there can be no information security. Individual accountability is required when accessing all University resources, and includes:
   i. access to University computer systems and networks must be provided through the use of individually assigned unique computer identifiers, known as user-IDs;
   ii. individuals who use University computers must only access information assets to which he or she is authorized;
   iii. authentication tokens associated with each user-ID, such as a password, must be used to authenticate the person accessing the data, system or network. Passwords, tokens or similar technology must be treated as confidential information, and must not be disclosed. Transmission of such authentication information must be made only over secure mechanisms;
   iv. each individual is responsible to reasonably protect against unauthorized activities performed under his or her user-ID;
   v. User-ids and passwords (or other tokens or mechanisms used to uniquely identify an individual) must not be shared except where approved for group/shared small group accounts.

**4. Incident Management Process and Procedures:**

I. Information Security incidents will be logged and used by the University for regulatory purposes and to determine appropriate remediation and controls to limit the potential of future incidents.

II. **Incident Response Plan.** The Director for Information Security & CISO is responsible for developing and publishing an Incident Response Plan (IRP) for the University. That plan is available from CTS via request to help@duq.edu by University members.

III. Incident Response Team. The Incident Response Plan (IRP) will establish an Incident Response Team (IRT). This team is responsible for handling reported information security incidents for the University.

IV. **Reporting of Information Security Incidents**. Campus community members are to report any suspected or confirmed Information Security incident to the information owner, CTS Help Desk (help@duq.edu or 412-396-4357), the Director for Information Security & CISO or General Counsel. This includes but is not limited to viruses, spyware, malicious attack and activity, denial of service, breaches of confidentiality or the disclosure of restricted University data.

**5. Enforcement:**

The unauthorized or improper use of Duquesne University's technology environment, including the failure to comply with these service requirements, constitutes a violation which may result in the loss of access, University disciplinary actions and/or legal prosecution under federal, state and local laws, where applicable. Users are expected to adhere to T.A.P. 26 - Computing and Ethics Guidelines which can be found at http://www.duq.edu/taps.

The University reserves the right to amend these service requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws.

| Revision Date | Reason for Change | Author |
|---|---|---|
| 7/1/2018 | Annual review and update. | Tom Dugas, Chief Information Security Officer (CISO) |