Dixie State University Policy

463 Information Technology Security

I. Purpose

1.1 Dixie State University operates an extensive Information Technology infrastructure for the use and benefit of students, faculty, and staff and the fulfilment of its mission as an institution of higher education. The University also collects, creates, and utilizes information about its students and employees and internal operation. This policy defines the responsibilities and actions needed to maintain secure University information technology infrastructure, protect information held in trust by the University, and ensure that risk-based decisions regarding the use of information and technology infrastructure are made at the appropriate levels of University administration.

II. Scope

2.1 This policy will apply to all Dixie State University constituents who use, maintain, store or otherwise deal with information within the University information technology environment. This policy also applies to all University constituents who use or access university-owned, personal or third-party information technology resources to conduct University business or functions.

III. Definitions

3.1 ***Controlled Information***: Information for which there is a requirement or expectation that collection or creation of, access to, use, disclosure, and destruction of said information be protected and controlled at the University. Controlled information is defined in two categories, restricted and internal:

3.1.1 ***Restricted Information***: Information collected from or maintained about students, employees, alumni or other university constituents that is

confidential or private in nature. Additionally, other non-personal information may be considered restricted as defined by Federal/State law or contract. Access, use, protection and disclosure of restricted data are typically controlled by one or more of the following: Federal and State law or regulation, contract, and/or other applicable policies developed by the Utah System of Higher Education or Dixie State University. Examples of restricted information include, but are not limited to: any non-directory Family Educational Rights and Privacy Act (FERPA) information, Social Security numbers, medical records, individual passwords, personal financial data including bank account and credit card numbers, certain research data, or government-classified data. If stored with any of the preceding information elements in a record or if disclosed in an extraordinary or uncontrolled manner, information normally classified as directory information under FERPA, such as name, address, date of birth, major, class, etc. may also be considered restricted

3.1.2 ***Internal Information***: Information collected, processed, stored, or otherwise used by the University that is sensitive, proprietary, or otherwise expected to be kept confidential but is not otherwise classified or controlled as Restricted information. Access, use, protection and disclosure of internal data may be controlled by one or more of the following: Federal and State law or regulation, contract, and/or other applicable policies developed by the Utah System of Higher Education or Dixie State University. Examples of internal data may include but are not limited to: institutional financial records, research data, IT and facilities systems configuration information including passwords and digital keys, surveillance video, personnel records, or contracts and purchasing records.

3.2 ***Uncontrolled Information***: Information collected, processed, stored or otherwise used by the University for which there is no expectation of confidentiality nor any special protections or controls needed.

3.3 ***Critical Information***: Information that is required for continuing operation of the University and its critical functions. Failures or loss of critical IT resources could result in loss of critical university functions, create public safety issues, cause significant fiscal losses or incur legal liability.

3.4 ***Information Technology Resource (IT Resource)***: IT systems, infrastructure or media that provide essential services to core university functions or that display, process, transmit, store or otherwise utilize Information.

3.4.1 ***Critical IT Resource***: IT resources that are required for continuing operation of the University and its critical functions. Failures or loss of critical IT resources could result in loss of critical university functions, create public safety issues, cause significant fiscal losses or incur legal liability.

3.4.2 ***Institutional IT Resources***: IT resources provided by University Information Technology Services or contracted third-party (also known as "Cloud") resources for the purposes of broad institutional use. Examples include the campus network, Banner system, email system, electronic directories, storage, Dixie State University Web site, any contracted third-party equivalents, and various other servers and infrastructure.

3.4.3 ***Personal IT Resource***: Any IT resource not owned or otherwise provided by the University.

3.4.4 ***Portable Devices and Media***: An IT resource used to display, process, transmit or store data that is easily portable. Examples include but are not limited to laptop computers, smartphones, tablet computers, optical media, magnetic tapes, removable hard drives, flash memory devices (USB thumb drives, memory cards) and other portable devices with storage capabilities.

3.5 ***Information Security Office:*** The Information Security Office (ISO) is responsible for developing and coordinating institutional Information Security strategies.

3.6 ***Data Steward***: An administrative position responsible for a University unit or department, typically a vice-president, a direct report to a vice-president, or an appropriate deputy designated to act in that capacity. The Data Steward is the principal IT security decision-maker and is responsible for the acceptance of risk and other matters regarding Information Security for controlled information collected, stored, or used within the scope of their authority.

3.7 ***Data Custodian***: Any employee or other authorized affiliate with administrative or operational access to Controlled information and/or IT Resources as part of their normal job functions.

3.8 ***Users***: Any University employee or other affiliate who accesses and uses University information assets and IT resources.

3.9 ***Incident Response Team***: The Incident Response Team is a group convened when ISO determines the scope, size, or nature of an Information Security

incident warrants additional response resources. The Incident Response Team is coordinated by ISO and may be comprised of Data Custodians, institutional and/or third-party subject-matter experts and other stakeholders as deemed appropriate for the incident.

3.10 ***Disaster***: Any unexpected event or occurrence that prevents the normal operation or causes the loss of one or more Critical IT Resources.

3.11 ***Disaster Recovery Plan***: A written plan covering provisions for implementing and running critical IT resources or equivalent alternative processing in the event of a disaster.

3.12 ***Unauthorized Access***: Access to controlled information or to IT resources by individuals or automated agents that are not authorized for access to perform job duties or university functions.

3.13 ***Branded Payment Cards***: Credit and debit cards issued by the major international payment brands, including but not limited to Visa, MasterCard, American Express, Discover.

IV. Policy

4.1 Roles and Responsibilities

4.1.1 Each Data Steward, for information or resources within his/her respective area of control, shall be responsible to:

4.1.1.1 Determine the classification, as defined by this policy, of Information Assets under his/her control.

4.1.1.2 Determine the criticality of Information Assets and IT Resources.

4.1.1.3 Maintain an inventory of the uses of Restricted information collected, stored, used, or transmitted in his/her area of control.

4.1.1.4 Advised by the Information Security Office, evaluate threats and risks to Controlled Information and act as the primary decision maker for use of Controlled information. Authorize access to and use of Controlled Information within his/her department or unit, or delegate authorization responsibilities to an appropriate deputy.

4.1.1.5 Take appropriate steps to ensure critical information or IT resources under his/her area of control remain available or recoverable in the event of a loss or interruption due to a disaster

or other adverse event.

4.1.1.6 Assist in enforcement of institutional information security practices within his/her area of control.

4.1.1.7 Authorize and accept responsibility for any exceptions to institutional security practices as defined by this policy and attached procedures.

4.1.2 Each Data Custodian, for information or resources within his/her respective area of operation shall be responsible to:

4.1.2.1 Understand the classification of information he/she is administratively or operationally in custody of and follow institutional information security practices appropriate to that classification.

4.1.2.2 Ensure that decisions on access to and use of Controlled Information are made by the appropriate Data Steward or delegated deputy.

4.1.2.3 Release Controlled Information only through appropriate, established channels.

4.1.2.4 Assist Data Stewards in inventorying use of Restricted data collected, stored, used, or transmitted on resources in his/her area of operation.

4.1.2.5 Report any unauthorized access or suspected security incident/breach to ISO in a timely manner.

4.1.3 The Information Security Office shall be responsible to:

4.1.3.1 Develop and maintain institutional information security policies and practices in coordination with Data Stewards and Data Custodians.

4.1.3.2 Educate and provide assistance in complying with this policy to Data Stewards, Data Custodians and Users.

4.1.3.3 Operate or coordinate appropriate security measures for protection of institutional information technology infrastructure.

4.1.3.4 Monitor network traffic to identify, evaluate, and mitigate threats or vulnerabilities to University Controlled information or

resources, and to assess compliance with institutional security policies and practices.

4.1.3.5 Take appropriate and reasonable action to resolve security incidents. Direct incident response activities and incident resolution including convening the University Information Security Incident Response Team if necessary.

4.1.3.6 Conduct periodic security assessments to identify evolving threats and vulnerabilities to the security of institutional information and infrastructure, and to evaluate compliance with information security policies and practices.

4.1.3.7 Enforce institutional security policies and practices in coordination with Data Stewards

4.1.4 Users shall be responsible to:

4.1.4.1 Understand and follow University policies and practices governing the use of Institutional IT resources and Controlled information.

4.1.4.2 Report any unauthorized access or suspected security incident/breach to ISO in a timely manner.

4.1.5 The Incident Response Team, when convened, shall be responsible to:

4.1.5.1 Under the direction of the ISO, contain and resolve security incidents as directed by the Information Security Incident Response Procedures.

4.2 Protection of Controlled Information

4.2.1 Controlled information, defined at DSU as Restricted and Internal information, must be protected in all phases of its lifecycle, including creation/collection, use, storage, transmission, and disposal such that the Controlled information remains confidential.

4.2.1.1 Controlled information must not be disclosed or released except through channels and procedures established by the appropriate Data Steward(s).

4.2.2 Restricted information must not be moved, or copied from, or stored

anywhere other than Institutional IT resources, including but not limited to workstations, portable computing devices or media, personally-owned devices, or third-party "cloud" services not deemed an Institutional IT resource.

Using a workstation or other device to enter, view, or manipulate Restricted information stored on an Institutional IT resource is permitted so long as the Restricted information is not moved, copied, or stored on the viewing workstation or device.

Exceptions may be approved in the following circumstances:

4.2.2.1 There is a business need for Restricted information to be stored, moved, or copied from Institutional IT resources that cannot otherwise be met.

4.2.2.2 The Data Steward(s) over the Restricted information in question must be made aware of request for exception, be apprised of any risks in granting an exception, and approve of the departure from standard practice.

4.2.2.3 An inventory of the nature and of the Restricted information, the location or disposition of the information, and the number of records must be maintained by the department or unit.

4.2.2.4 Appropriate, documented, and auditable protections for the Restricted information are in place following the guidelines established in procedure Information Protection Practices.

4.2.2.5 Faculty members do not require permission from a Data Steward to maintain records of grades outside of institutional resources, but if doing so, must protect that information appropriately following the guidelines established in procedure Information Protection Practices.

4.2.3 Access to Controlled information should only be granted for individuals and entities who need access to perform their designated job function, contracted services on behalf of the University, or to meet some other regulatory or legal requirement. Data Stewards and/or their designated deputies must authorize access to Controlled information.

4.2.4 A third-party or "cloud" service may be considered an institutional IT resource suitable for collection, use or storage of Controlled information when an appropriate contract is in place that protects the University's

interests and outlines security measures to be taken on the part of the third-party provider. When possible, administrative access to and control of information held in trust by the third-party provider should available to University Information Technology Staff. Integration with the University DixieID identity and authentication systems must also be used whenever possible.

4.2.5 Refer to procedure Information Protection Practices for current minimum measures that must be taken to protect Controlled information.

4.2.6 Industry regulation of branded payment cards impose additional security requirements for University departments or other units accepting branded payment cards. These requirements are defined by the Payment Card Industry Data Security Standards. Before conducting commerce or otherwise collecting University funds using branded payment cards, departments and units must be granted approval from University Business Services. Departments and units accepting branded payment cards must adhere to practices developed to protect credit card holder information as required by the University Cash Handling policy, currently published PCI-DSS standards, and internal requirements and guidance maintained by the University Payment Card Committee.

4.3 Protection of Critical information and IT resources

4.3.1 Information or IT resources that have been deemed critical by the responsible Data Steward(s) should be appropriately protected from loss through equipment failure, natural or human-caused disaster, malicious destruction, or other adverse events such that the information or resource can be restored to an operational state.

4.3.1.1 University Information Technology Services shall develop means to protect institutional critical information stored and used on either local resources it maintains or on third-party hosted (aka "Cloud") solutions it coordinates. Departments and other units using institutional IT resources may coordinate with Information Technology Services to ensure that critical information is appropriately protected.

4.3.1.2 Departments or units maintaining critical information outside of institutional resources provided or coordinated by Information Technology Services (e.g. on individual workstations or on third-party hosted solutions, aka "Cloud" services) must ensure that

critical information is appropriately protected from loss.

4.4 Reporting and handling of IT Security Incidents

4.4.1 All suspected or actual IT security incidents involving institutional or departmental information must immediately be reported to the Information Security Office.

4.4.2 ISO is authorized to take or direct reasonable action as necessary to neutralize a security incident or prevent further damage, including but not limited to disabling user accounts, blocking network traffic and disabling services.

4.4.3 ISO will coordinate response, investigation and reporting of information security incidents as defined in procedure Information Security Incident Response. If necessary, ISO will convene the Incident Response Team to assist in handling the incident. ISO and/or the Incident Response Team work to contain or mitigate any unresolved threat stemming from the incident to IT resources or information assets. ISO and/or the Incident Response Team reports findings and recommendations regarding the incident to University administration and appropriate Data Stewards.

4.4.4 If it is determined that University constituents must be notified of disclosure or loss of Controlled information, efforts must be coordinated between responsible Data Stewards, ISO, University legal counsel, University public relations and other stakeholders as necessary to ensure that notification is performed by the responsible Data Steward in a timely manner in accordance with Federal and State notification laws and regulations.

4.5 Reporting loss of critical IT Resources – If critical IT resources or information assets are lost or inaccessible due to disaster or system failure, the Data Steward and/or Data Custodian(s) responsible must notify those individuals and organizations within the University that are affected by the loss of the resource.

4.6 Physical Information Security – University departments and units are responsible for assuring that all Controlled information, whether in digital or physical format and technology infrastructure are physically protected at all times in accordance with their level of criticality and sensitivity. University departments and units must assure that the physical information security controls for work area are followed and that access restrictions, Controlled information security practices and physical security practices for each area are adhered to.

4.7 Destruction or sanitization of electronic media – Departments and University units shall destroy or otherwise sanitize Controlled Information stored on a university or personally-owned IT resource when the information is no longer necessary to conduct the business of the University or meet regulatory requirements, or when hardware or media devices are retired or repurposed. Refer to procedure Information Protection Practices.

4.8 Additional procedure and practices – This policy authorizes Data Stewards, Data Custodians, ISO, and Information Technology Services to develop additional Information Security procedures and guidance in accordance with the requirements and intent of this policy. Data Stewards may implement rules for the departments or units for which they are responsible.

4.9 Revocation of Access

4.9.1 Dixie State University shall reserve the right to revoke access to the DSU network or any IT resource for any internal or external user, device, network segment or system which presents a direct and imminent threat to University IT resources or information assets, violates this policy, attached procedures or established practices or for any other reason in accordance with applicable institutional policies.

4.9.2 Restoration of Access – Access for a revoked user, device, network segment or system may be restored as soon as the direct and imminent security threat or policy violation has been remedied.

4.10 Policy Violations

4.10.1 Violation of this policy may result in action in accordance with University disciplinary policies.

4.10.2 University constituents may appeal revocation of access to IT resources or disciplinary actions taken against them pursuant to University grievance policies.

V. References

5.1 Utah System of Higher Education, Policy R345, Information Technology Resource Security

5.2 Dixie State University of Utah Policy 372 Corrective & Disciplinary Action

5.3 Dixie State University of Utah Policy 151 Grievance Procedure

VI. Procedures

6.1 TBA – Data Protection Practices

6.2 Incident Response

VII. Addendum

7.1 Information Classification Matrix

		Examples	Controls
Controlled Information	**Restricted Information** **RED**	• Non-directory FERPA information • Social Security Numbers • Personal Financial Data (e.g. credit cards and bank accounts) • Health Records • Other personal information with a requirement or expectation to maintain confidentiality	• Always controlled, typically by Federal/State laws and regulations or through contract. • Assigned University Data Steward owns and must approve all uses of Restricted information. • May not be copied or stored outside Institutional IT Resources without permission from Data Steward. • Must be appropriately protected in all phases of collection, storage, processing, and disposal. • May be public disclosed in rare circumstances, always through proper channels; no uncontrolled release.
	Internal Information **YELLOW**	• Institutional financial records • Contracts / purchasing data • Institutional / departmental plans and other records • IT / Facilities system configurations • Other proprietary University information with a requirement or expectation to maintain confidentiality	• May be controlled by Federal/State laws or through contract. • Assigned University Data Steward owns all uses of Internal information. • Must be appropriately protected in all phases of creation/collection, storage, processing, and disposal. • May be publicly disclosed in certain circumstances through proper channels; no uncontrolled release.
	Uncontrolled Information **GREEN**	• Public Web information • Course Catalog • All other University information	• Uncontrolled information. No expectation of confidentiality or special protections required.

Policy Owner: VP Administrative Services

History:
Approved 4/28/2017