Dixie State University Policy

462 Use of University Information Technology Resources

I. Purpose

1.1 Dixie State University owns, maintains, and makes available Information Technology Resources for authorized use. These Information Technology resources and information assets are intended to support the mission of the University. This policy will outline the use of University Information Technology Resources.

II. Scope

2.1 This policy applies to all users of Dixie State University Information Technology resources and governs all Information Technology systems owned or leased by the University, whether individually controlled or shared, stand-alone, or networked.

III. Definitions

3.1 ***Access Credentials***: Usernames, passwords, tokens, or any other credential or identifier that has the purpose of verifying the identity and authorization of a user to access and perform tasks using an IT resource.

3.2 ***Chief Information Officer (CIO):*** The senior administrative authority regarding operation and development of Information Technology resources and IT support services for Dixie State University.

3.3 ***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.

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

3.5 ***Enterprise Email:*** An enterprise email service provided by the University which is intended for use by employees, officers, and other designated affiliates of the University for institutional email communications. This service provides addresses with a @dixie.edu suffix. The definition of enterprise email service does not extend to separate, additional email services that may be offered to other University groups such as students, alumni, and emeritus employees; for example, @dmail.dixie.edu addresses.

3.6 ***Information Technology Governance Committee (ITGC)***: Reviews and recommends new Information Technology policies and procedures, and changes to existing policies and procedures. Assists the University CIO and Data Stewards in reviewing and prioritizing IT projects and initiatives.

3.7 ***Information:*** Per the categories defined in DSU Policy 463: Information Technology Security, information or data collected, processed, maintained, stored or otherwise used by Dixie State University in electronic form to conduct core university functions.

3.8 ***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.

3.8.1 ***External IT resources*****:** Systems, services, networks, and media not owned or controlled by the University, including Internet resources, that are made accessible via University networks and services.

3.8.2 ***Institutional IT Resources:*** IT resources provided by University Information Technology Services, contracted third-party (also known as "Cloud") resources, or resources not owned by the University but paid for by University funds for the purposes of institutional business and use. Examples include but are not limited to the campus network, Banner system, email system, electronic directories, storage, Dixie State University Web site, any contracted third-party equivalents, mobile devices including phones, workstations, and various other servers and infrastructure.

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

3.9 ***University Information Technology Services (ITS):*** The University Services department responsible for the operation and development of institutional IT services under the direction of the University CIO.

3.10 ***User***: Any student, employee, affiliate, or guest who accesses or uses University information assets and IT resources.

IV. Policy

4.1 Access to University owned or operated Information Technology Resources – The University owns and/or operates its IT resources and information assets and reserves the right to govern the use and availability thereof.

4.1.1 Access to University IT resources and information assets is granted to authorized users subject to University and Utah System of Higher Education policies, and local, state, and federal law. Use of any University IT resource(s) indicates that the user agrees to and must abide by the laws and policies governing such use. Users unwilling to abide by these terms of use may have IT privileges revoked.

4.2 Non-University Business and Personal Use of University IT Resources

4.2.1 Use of University IT resources to conduct business or work unrelated to University employment or duties individually and/or on behalf of external entities is restricted.

4.2.2 Incidental personal use of University IT resources by employees must not impede the performance of their job responsibilities or the job responsibilities of other employees. Personal use of enterprise email by employees is permitted, but not encouraged. Employees should be aware that open records statutes and other privacy implications outlined in section 4.6 of this policy may impact any personal use of University IT resources.

4.2.3 Use of University IT resources through joint-ventures, economic development programs, or other arrangements between the University and external entities must be approved by University Administration, including the University CIO. Use of University IT resources in such circumstances will be governed by all applicable University policies and any agreements negotiated by the University with participating entities.

4.3 Use of non-University owned devices – The University permits the use and/or connection to the University IT network of computing and storage devices

owned by students, staff, faculty, and other University affiliates and third-parties. Non-University-owned devices must comply with all University IT policies, rules, and standards governing the use thereof. Use of non-University owned devices used by University employees to conduct official University business with confidential personal or internal information must meet the criteria outlined in DSU Policy 463: Information Technology Security. The University reserves the right to refuse use and connection privileges to any device at any time.

4.3.1 Use of any University IT resource or connection to the University network by a non-University owned (i.e. personally-owned) device indicates that the user agrees to comply with this policy and any associated rules, standards, procedures, and acceptable use agreements governing the use of University IT resources by non-University-owned devices.

4.4 Use of Enterprise Email to conduct University Business – Utah State System of Higher Education Policy R840 imposes policy requirements regarding institutional email communications. All employees, officers, and other designated affiliates of the University must use their assigned *@dixie.edu* enterprise email address to conduct University business by email.

4.4.1 Use of any private, personal, or non-enterprise email service to conduct University business is prohibited. Automated forwarding of all University email to a private, personal, or non-enterprise email address is also prohibited.

4.4.2 Use of third-party mass-mailing services in conjunction with the enterprise email service to conduct University business is permitted so long as these services are registered with University IT Services. Registration ensures that these services are compatible with the University enterprise email system.

4.5 Access Privileges – Students, faculty, staff, and other University affiliates may be granted access privileges to various IT resources and authorization privileges to perform tasks within those resources. Access and authorization privileges for University IT resources are governed by procedures established by data stewards, the ITGC, or University ITS. Users must follow these procedures when seeking access and authorization privileges. The University reserves the right to suspend or revoke access privileges. Users are not authorized to transfer or confer these privileges to others.

4.5.1 Users are assigned unique identifiers and accounts, and users are accountable for activities that take place using their usernames, passwords, or other access credentials.

4.5.2 Students, faculty, staff and other users will not share or disclose their usernames and passwords and other access credentials to DSU IT resources to co-workers, fellow students, or other parties.

4.6 Expectation of Privacy – The University strives to maintain an IT environment that values academic freedom and the privacy of its users using University IT resources. Users shall respect the privacy of others by making no attempts to view or access University data or the private data of other users transmitted and/or stored by University IT resources unless explicitly authorized. However, users should not expect complete privacy in their use of University IT resources. No computing system is entirely without risk. Therefore, the University makes no guarantee that data stored on or transmitted by University IT Resources can be completely protected from disclosure or unauthorized access. The following include, but are not limited to, circumstances which may affect a user's expectation of privacy for data viewed, transmitted, or stored on University IT resources:

4.6.1 The University reserves the right to access any University-owned information stored on University-owned or provided devices and IT resources at any time.

4.6.2 The University will cooperate with court orders, search warrants, subpoenas, and other requests for information under Utah State and Federal laws and regulations.

4.6.3 As a publicly-owned institution, the University is subject to Utah State public records laws. This may result in disclosure of information including but not limited to the email messages and documents of University employees, regardless of any expectation of privacy. Classification and release of information relating to public records requests is controlled solely by the University Office of General Counsel.

4.6.4 University Data Stewards and Data Custodians, including ITS staff, have administrative privileges over IT resources. These individuals may have access to information contained within or transmitted by these resources as necessary to perform their job responsibilities. Additionally, users may request technical assistance regarding

computer systems and accounts from University IT administrators and technical support staff. Administrators and technical support staff engaged in a good faith effort to assist the user may view or access material for which the user has an expectation of privacy.

4.6.5 University ITS staff routinely engages in automated and manual monitoring of system activity and network traffic to measure performance, identify problems, and detect and investigate IT security events.

4.7 Acceptable use and individual responsibilities in maintaining a professional and academic environment – Users of University IT resources have a responsibility to maintain an Information Technology environment conducive to the mission of the University.

4.7.1 The University expects users to maintain a secure IT environment that values both academic freedom and integrity.

4.7.1.1 Users will not gain, attempt to gain, or help others to gain unauthorized access to University or external IT resources.

4.7.1.2 Users will not engage in actions that intentionally cause University or external IT resources to be unavailable, degraded, or otherwise compromised.

4.7.1.3 Users will not circumvent or subvert IT policies or technical controls of University or external IT resources.

4.7.1.4 University IT resources shall not be used to illegally obtain, store, distribute, or otherwise use copyrighted software, media , or other content.

4.7.1.5 Users will not excessively consume, monopolize, or waste University IT resources.

4.7.1.6 University IT resources will not be used to originate or distribute unsolicited bulk messages that do not pertain to University business.

4.7.1.7 Users will not use University IT resources to directly or indirectly harass others or create a hostile environment as defined by DSU policy 154 Title IX, Harassment and Nondiscrimination.

4.8 This policy authorizes Data Stewards, ITGC, The University CIO and

University ITS 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.

V. References

5.1 Dixie State University Policy 372: Corrective & Disciplinary Action

5.2 Dixie State University Policy 463: Information Technology Security

5.3 Dixie State University Policy 157: Personal Conduct/Conflict of Interest

5.4 Dixie State University Policy 154: Title IX, Harassment and Nondiscrimination

5.5 Dixie State University Policy 552: Student Conduct Code

5.6 Utah System of Higher Education Board of Regents Policy 840: Institutional Business Communications

VI. Procedures

VII. Addenda

Policy Owner: Vice President of Administrative Affairs
Policy Steward: Chief Information Officer/Information Security Officer

History:
Approved 05/07/10
Revised 02/01/19
Revised 01/31/20