Appropriate Use of Information Technology Resources Policy

University information technology (IT) resources are a valuable community asset provided to eligible employees, students, and other individuals for purposes related to the university's mission of teaching, learning, research, creative activity, and appropriate university business activities. As such, they are to be used and managed responsibly to ensure their integrity, security, and availability.

This policy prescribes the appropriate use of Brigham Young University's IT resources.

Access to university IT resources is limited to university employees, students, and others authorized by the university and may be subject to legal, ethical, and university requirements.

Definitions

Information Technology Resources (IT Resources) means university-owned infrastructure, cloud services, software, and hardware with computing and/or networking capability. It includes, but is not limited to, computers, computer systems, telephones, tablets, mobile devices, classroom presentation systems, voice communications and messaging equipment, networks and networking systems, radio communications equipment, computer software, electronically stored institutional data and messages, all similar resources, and any additional technologies or services instituted to maintain these resources.

Information Technology Standards (IT Standards) means minimal controls to address identified risks to the confidentiality, integrity, and availability of university systems, data, and resources. (*See* BYU Information Technology Standards.)

Personally Owned Data means data that was not created or acquired by a university employee or campus unit for institutional purposes but belongs to an individual. Personally Owned Data includes, but is not limited to, income tax, medical, banking, financial, family, or other personal information or data that an individual might reasonably assume to be private or sensitive.

Ownership

The university retains absolute ownership rights of IT Resources. IT Resources leased, licensed, or purchased under research contracts or grants are administered under the terms of this policy for as long as they remain within the lawful possession or control of the university.

Terms of Use

As a condition to accessing and using IT Resources, all users must

- comply with all applicable laws, university policies and procedures, contracts and licenses, and the Church Educational System Honor Code;
- use only those IT Resources that the individual user is authorized to use and only in the manner and to the extent authorized;
- not attach any device that may, in any way, endanger or disrupt the continuous and stable operation of the university network or other IT Resources, or that may compromise the confidentiality or integrity of information stored on any technology resource;
- not share or transfer individual university accounts, including network IDs, passwords, or other access codes that provide access to IT Resources;
- respect the privacy of other users and their accounts, devices, and data regardless of whether those elements are securely protected; and
- respect the limitations of IT Resources and manage usage to not interfere with the activities of others.

IT Standards

To protect university systems, data, and resources, all users of IT Resources must adhere to the IT Standards.

The assistant vice president(s) of information technology and the chief information security officer, under the direction of the chief information officer and with input from the Information Technology Policy Committee, create, approve, and update the IT Standards.

Personal and Commercial Use of IT Resources

IT Resources may be used for incidental personal and ecclesiastical purposes. Personal or ecclesiastical use of IT Resources must not occur under circumstances that interfere with employee work responsibilities, displace other IT Resources, or require purchases of additional IT Resources. (*See* Conflict of Interest Policy.)

Users must not use IT Resources for non-university commercial purposes or non-university gain, unless authorized in writing by the individual user's responsible vice president and the university's chief information officer.

Privacy and Monitoring

The university provides no general expectation of privacy in the use of IT Resources except as required by law.

BYU reserves the right to monitor and report technology use, including the use of personal devices connected to IT Resources, to the maximum extent permitted by law. All users, by their use of IT Resources, consent to such monitoring and reporting.

As permitted by law, the university may disclose to third parties data residing in IT Resources.

Reporting

All members of the university community must promptly report the following to the CES Security Operations Center:

- known or suspected breaches of data or compromises of IT Resources
- abnormal or systematic unsuccessful attempts to compromise the university's data or IT Resources
- any suspected or actual weaknesses in the safeguards protecting data or IT Resources

The BYU Information Security Major Incident Response procedure outlines and guides the university's incident response.

Lost or stolen university-owned devices such as desktops, laptops, tablets, portable storage devices, and mobile phones should be reported as soon as possible to BYU Risk Management.

Revocation

The university reserves the right, in its sole discretion and for any reason or no reason, to immediately revoke authorization to access or use any or all IT Resources.

Sanctions

Employees and students who commit a violation of this policy may be subject to disciplinary actions by the university and may also be prosecuted under applicable local, state, or federal civil or criminal law. University disciplinary actions may range from counseling to dismissal, consistent with university disciplinary policies.

Disclaimers

Users use IT Resources at their own risk. Although the university makes reasonable efforts to secure its IT Resources, and strives to make its IT Resources effective and efficient, it cannot guarantee their confidentiality, integrity, and availability. The university makes no warranty or promise that IT Resources will operate as designed or as expected by the user. University IT professionals are not available to recover any Personally Owned Data that is lost or compromised. The university assumes no legal responsibility for any damages or losses of any kind, including but not limited to loss of Personally Owned Data or devices, arising from the failure of IT Resources. Users can minimize the risk of data loss by always backing up their data.

APPROVED: 26 Feb 2024

PRIOR VERSION: 27 Dec 2023

APPLICABILITY: This policy applies to all individuals and entities who maintain or use IT Resources.

POLICY OWNER: Information Technology Vice President and CIO

RESPONSIBLE OFFICE: Office of Information Technology

IMPLEMENTING PROCEDURES: BYU IT Standards, Computer Tracking

RELATED POLICIES:
- Church Educational System Honor Code
- Conflict of Interest Policy
- Copyright Policy
- Data Use, Privacy, and Security Policy
- Network Resources Policy