Information Use, Privacy, and Security Policy

Brigham Young University strives to maintain standards and practices that protect the privacy and security of the information of its students, faculty, and staff that it controls, in accordance with ethical, contractual, and legal requirements for information use, privacy, and security.

Definitions

Data Steward means an employee with designated responsibility for the processes that generate, receive, distribute, store, use, and share a specific domain of data.

Nonpublic Institutional Data means any information created, controlled, owned, or stored by the university, except for information that is publicly published or available.

Personal Information means any information that relates to, is associated with, describes, identifies, or can reasonably be used to identify a natural person.

Access to Nonpublic Institutional Data

Access to Nonpublic Institutional Data is limited to the following:

- An individual (e.g., student, alum, employee, donor, patient, patron) may access his or her own Personal Information, subject to applicable laws and BYU policies.
- A university employee may access and use Nonpublic Institutional Data as necessary for legitimate university purposes associated with his or her job, provided that the employee uses authorized university systems and processes, including approval by the assigned Data Stewards to ensure (i) appropriate use of the data to support university purposes, (ii) the confidentiality and privacy of those individuals whose records may be accessed, and (iii) compliance with applicable laws or policies with respect to access, use, and disclosure of the data.
- A third party (e.g., external agency, consultant, contractor, vendor) may access and use Nonpublic Institutional Data only when the third party's access and use of the data is (i) for legitimate university purposes, (ii) approved by the assigned Data Stewards, and (iii) subject to a written agreement between the third party and BYU requiring the third party to take measures to appropriately safeguard and use the information pursuant to BYU policy and applicable laws.
- Nonpublic Institutional Data may be disclosed in certain legal proceedings (e.g., lawfully issued subpoenas, warrants, and court orders) under the direction of the Office of the General Counsel. All subpoenas, warrants, and court orders must be referred to the Office of the General Counsel immediately upon receipt.

Collection, Use, Disclosure, Storage, and Disposal of Nonpublic Institutional Data

The collection, use, disclosure, and storage of Nonpublic Institutional Data is limited to that which reasonably serves the university's academic, research, administrative, or other legally required purposes. Such collection, use, disclosure, and storage must comply with applicable university policies and relevant state, federal, and foreign laws, rules, and guidelines. Additionally, Nonpublic Institutional Data must be promptly and securely disposed of in accordance with BYU's Information and Records Retention Policy.

Information about how BYU collects, processes, uses, and protects Personal Information can be found in the BYU Privacy Notice.

General Principles on the Collection and Use of Personal Information

The following general principles apply to the collection and use of Personal Information:

- The collection and use of Personal Information should be open and transparent to the subject individual.
- Personal Information should be accurate, complete, and relevant to the purposes for which it was collected.
- Individuals should be allowed to inspect and correct their Personal Information as required by law.
- The purpose for collecting Personal Information should be described at the time the specific Personal Information is collected. Only information necessary for the stated purpose should be collected. Any further use of the information should be limited to the purpose described at the time of collection. Personal Information should not be disclosed for secondary purposes without the consent of the subject, unless required by law, and should be securely destroyed or deleted when no longer needed for the defined purposes in accordance with BYU's Information and Records Retention Policy.
- Access to Personal Information that is not publicly available should be limited to those employees with a specific need to access the information to accomplish the functions of their respective jobs.
- Personal Information that is not publicly available should be protected by reasonable security safeguards approved by the assigned Data Steward against reasonably anticipated risks, such as loss, unauthorized access, destruction, use, modification, or disclosure.

Privacy on Campus

The university uses video surveillance in public locations on campus for safety and security purposes. To protect the privacy of individuals on campus, photography, video recordings, and recordings for other purposes may be made only in accordance with university policy, including the Filming and Photography on Campus Policy. Monitoring of IT resources must comply with the Appropriate Use of Information Technology Resources Policy.

Information Governance, Privacy, and Security Procedures

Information governance, privacy, and security procedures supporting this policy must be based on the following principles:

- The appropriate use, privacy, and security of Nonpublic University Information are responsibilities that extend to all university personnel, processes, and activities.
- Data Stewards are responsible for ensuring that data is generated, received, distributed, stored, used, and shared in a manner compliant with BYU policies and procedures, as well as applicable laws.
- Information governance procedures provide organizational focus, consistency of approach, and resources for Data Stewards across the university.
- The senior director of information governance, the chief information privacy officer, and the chief information security officer, under the direction of the chief information officer and with input from relevant stakeholders, create and approve information governance, privacy, and security procedures for the university that apply to every organizational unit of the university, unless specifically indicated.

Reporting Requirements

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

- Known or suspected breaches of information or information technology security;
- Abnormal or systematic unsuccessful attempts to compromise the university's information or information systems;
- Any suspected or actual weaknesses in the safeguards protecting information or information systems; and
- Lost or stolen university-owned devices such as desktops, laptops, tablets, portable storage devices, and mobile phones.

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

APPROVED: 1 Mar 2021

PRIOR VERSION: 2 Oct 2017

APPLICABILITY: This policy applies to all members of the university community, visitors, affiliates, and business associates including students, faculty, staff, lecturers, instructors, third-party vendors, and any others with access to university information and all persons, systems, and activities where Nonpublic University Information is stored, processed, or transmitted in either electronic or printed form.

POLICY OWNER Information Technology Vice President and CIO

RESPONSIBLE OFFICE: Office of the Chief Information Security Officer

IMPLEMENTING PROCEDURES:

- BYU Information Security Major Incident Response
- BYU Student Health Center Privacy Practices
- Information Privacy Standard

RESOURCES:

- BYU Info Hub
- BYU Information Security and Privacy

RELATED POLICIES:

- Access to Student Records Policy
- Appropriate Use of Information Technology Resources Policy
- Filming and Photography on Campus Policy
- Human Research Protection Policy
- Information and Records Retention Policy
- Merchant Credit Card Policy
- Network Resources Policy
- University Archives Policy