Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Office of the President
Implementing Authority: Vice President for Administration and Finance
Effective Date: June 2024
Review: May 2025

Access to Personal and Confidential Information - Policy & Procedures

1.0 Purpose

1.1 The purpose of this policy is to establish guidelines and procedures for granting, managing, and restricting access to personal and proprietary information held by AUIB.

2.1 This policy aims to safeguard and protect the privacy rights of individuals and proprietary information of the university. Everyone has the right to the protection of personal data concerning him or her and access to data which has been collected concerning him or her, and the right to have it rectified.

2.0 Scope

2.1 This policy applies to all university employees, students, contractors, volunteers, and any other individuals granted access to personal and proprietary information in the course of their duties or affiliation with the University.

2.2 This policy covers all university data, regardless of the technology or method used for retaining, storing, or processing this data.

2.3 This policy covers all university-related proprietary information and personal data.

3.0 Definitions

3.1 Access - the ability to view, modify, or interact with personal and proprietary information.

3.2 Data Steward - The individual designated by the Vice President for Academic Affairs, (VPAF), as custodian of a specific category of data.

3.3 Personal Information - Any information that relates to an identified or identifiable living individual. Different pieces of collected information, once taken together, can lead to the identification of a particular person, and also constitute personal data. Examples include a name and surname, a home address, a national identification number, phone number, passport number, financial information, or medical records.

3.4 Proprietary Information - Data that pertains to the operation of the university and is sensitive in nature and requires protection to prevent unauthorized access or disclosure. This includes information designated as proprietary.

4.0 Policy

4.1 Access to personal and proprietary information will be granted solely on a need-to-know basis, limiting it to individuals whose job responsibilities require access to perform their duties effectively.

4.2 The university will implement appropriate technical, physical, and administrative safeguards to protect personal and proprietary information from unauthorized access, disclosure, alteration, or destruction.

4.3 Access to personal and proprietary information shall be granted based on job roles and responsibilities, and only after appropriate authorization by the relevant data owner or data custodian. Access will be granted at the minimum level necessary to carry out specific job functions and responsibilities.

4.4 Individuals with access to personal and proprietary information are accountable for the protection and appropriate use of the data they handle. Sharing of access credentials, passwords, or any other means of authentication used to access confidential information is strictly prohibited.

4.5 Persons who suspect or have knowledge of unauthorized access to personal or proprietary information must be immediately reported to the Vice President for Administration and Finance or other designated University authority.

4.6 Upon termination of employment or affiliation with the university, individuals' access to personal and proprietary information will be promptly revoked.

4.7 In case of data breaches or unauthorized disclosures, the university shall follow a pre-established incident response plan to mitigate the impact and take corrective actions.

4.8 Access to personal and proprietary information will be subject to periodic reviews, audits, and monitoring to ensure compliance with this policy.

4.9 Regular training and awareness programs will be conducted to educate personnel about the importance of data privacy, security, and the proper handling of personal and proprietary information.

5.0 Procedures

5.1 Access to personal and proprietary information shall be requested by the relevant department or individual through an official Access Request Form.

5.1.1 The Vice President of Administration and Finance (VPAF) will create an Access Request Form which must include the justification for access, the specific information required, the duration of access needed, and approval from the data owner or data custodian.

5.1.2 The Access Request Form shall be reviewed and approved by the designated Data Steward responsible for the respective data category.

5.1.3 The Data Steward(s) will grant access to authorized personnel and define the access privileges based on the principle of least privilege.

5.2 The Director of Information Technology shall implement technical measures to control access to personal proprietary information, including user authentication, encryption, and access controls.

5.3 All personnel with access to personal and proprietary information shall undergo mandatory training on data privacy, security best practices, and their responsibilities under this policy.

5.4 Any suspected or actual unauthorized access to personal or confidential information must be reported immediately to the VPAF or other designated university authority.

5.4.1 The VPAF will convene a representative investigative committee to promptly investigate the reported incidents, take appropriate corrective actions, and document the incident response process.

5.4.2 The VPAF will ensure that all investigative committee members are trained in the relevant policies and procedures.

5.5 The VPAF shall regularly monitor access to personal and proprietary information and conduct periodic audits to ensure compliance with the policy and identify any potential security risks.

5.6 Access rights to personal and proprietary information shall be subject to regular reviews to ensure continued relevance and appropriateness.

5.6.1 Data Stewards shall conduct access reviews at least once every six months and ensure access rights are revoked for individuals who no longer require access due to job changes or termination.

5.7 The VPAF shall be responsible for updating the procedures document to reflect the needs of the university and its partners and seeking necessary approvals from university cabinet members. The VPAF shall designate and provide training for all data stewards.

Related Policies and Documents

Data Classification Policy
Information Security Policy
Acceptable Use Policy for Information Technology Resources
Code of Conduct for University Personnel
Access Request Form
Ethical Conduct and Safe Disclosure in Research
Incident Response Plan