INFORMATION SECURITY AND PRIVACY POLICY

Responsible Executive: CIO
Responsible Office: CIO
Date Issued: January 1, 2019
Date Last Revised: December 1st, 2019

CONTACTS

Title/Office	Telephone	Email/Webpage
Main Office	925-671-0121	info@urbanbarbercollege.com

Policy Clarification

STATEMENT OF POLICY

A trusted and effective information technology (IT) environment is vital to the Institution's ongoing mission of discovery, learning and engagement. To this end, the Institution will:

- Establish an overarching Information Security and Privacy Program to establish an environment of internal controls designed to maintain, facilitate and promote adequate protection of Information Assets and IT Resources through standards, procedures, guidelines, information-sharing and training.
- Identify and classify Information Assets and IT Resources according to their use, sensitivity, and importance to the Institution and in compliance with federal and/or state laws.
- Facilitate collaboration and communication among staff throughout the Institution's community to aid in protecting Information Assets and IT Resources, with recognition of the need to respond and adapt to rapidly changing and emerging technologies.
- Ensure that access to Information Assets via IT Resources is governed by appropriate role-based access controls and the principles of least privilege with Institution employees being granted access only to those Information Assets and IT Resources they need to fulfill the responsibilities of their position.
- Support the activities and responsibilities of Information Owners, Data Stewards and Data Users within the Institution's IT environment.
- Manage risk to Information Assets and IT Resources through appropriate administrative, technological and physical controls to protect both Information Assets and IT Resources from unauthorized access or modification, misuse or damage.

- Establish security and privacy controls meeting the requirements of legal, ethical, internally-imposed or externally-imposed constraints.
- Establish sanctions appropriate for non-compliance with control standards and procedures or for violation of applicable laws, regulations or other legal requirements.
- Conduct a periodic review of information security standards and procedures to maintain effective controls and relevance to changes in business processes, technology, applicable laws or regulations, and/or problems identified during risk assessments.
- Support, through the maintenance of an effective IT environment and the management of Information Assets and IT Resources for their maximum effective benefit, the Institution's ongoing mission.

  All individuals who use or have access to Information Assets and IT Resources, regardless of the user's role or affiliation with the Institution, are expected to act in accordance with this policy and its supporting Information Security and Privacy Program, as well as all relevant laws, contractual obligations and the highest ethical standards. Violations may result in disciplinary actions up to and including expulsion or termination or may be referred to appropriate external authorities.

REASON FOR THIS POLICY

Information Assets and IT Resources are essential to furthering the mission of Urban Barber College. These are Institution assets, or those entrusted to it by affiliates, that must be protected throughout various phases of their useful life, including when created or collected, stored, transmitted or transferred, and ultimately destroyed. To accomplish this objective, certain administrative, technological and physical safeguards must be in place to adequately protect Information Assets and IT Resources, while supporting their use in furthering Urban Barber College's mission. The Responsibilities outlined in this policy establish and define the organizational structure by which such safeguards are identified, promulgated, implemented and maintained.

INDIVIDUALS AND ENTITIES AFFECTED BY THIS POLICY

All individuals who use or have access to Information Assets and IT Resources are affected and governed by this policy and its supporting standards and procedures.

RESPONSIBILITIES

Vice President for Information Technology and System Chief Information Officer (CIO)

- Oversee the administration of this policy.
- Serve as Information Owner, or designate an Information Owner, for those enterprise-wide directories and applications that serve a multitude of Institution functions and do not have a cross-functional team that acts as the Information Owner. In these instances, the CIO or designee

is also responsible for identifying, communicating with and building consensus among all affected stakeholders whenever a decision regarding an Information Asset is needed.

- Lead, maintain and coordinate the organization-wide Information Security and Privacy Program, including associated standards and procedures to support the program controls and the common security controls among organizational entities.
- Ensure the Information Security and Privacy Program supports safeguards that protect information and respect privacy but does not impede the usage of information in the Institution's mission of discovery, learning and engagement.
- Ensure the Information Security and Privacy Program supports compliance with applicable state and federal laws and regulations and contractual requirements.
- Authorize the disconnection of any Device or the disabling of any account if it is believed that either is involved in compromising the information security of the Institution until such time as it is demonstrated that the Device or account no longer poses a threat; consult with agreed upon departmental or unit officials prior to disconnection, unless a critical situation exists (i.e., serious vulnerability, denial of service, worm or virus attack) and officials cannot be contacted quickly.
- Authorize the discontinuation of application development or deployment efforts if it is found during a risk assessment that the impact of a particular threat is likely to compromise the information security of the Institution with significant impact until a remedy is implemented to reduce or eliminate the impact of that threat.
- Guide information security strategy establish applicable policies and procedures, and review progress of the Information Security and Privacy Program.
- Steer the Information Security and Privacy Program in promoting technology, policy, awareness and remediation activities across the Institution.
- Communicate security concerns and security program requirements to their respective covered areas.
- Conduct risk assessments within their covered areas.
- Maintain an Information Asset inventory.
- Consult on the development of new policies, standards, security tools and techniques.

Data User

- Comply with standards and procedures for access and protection of Information Assets.

Data Steward

- Work with Information Owners to ensure that Information Assets are classified appropriately as it relates to their maintenance, use, protection and distribution.
- Establish procedures for maintaining Data confidentiality as they relate to Information Assets under the Data Steward's management. Work with security officers to enforce the procedures.

Information Owner

- Interpret and implement standards and procedures for access, availability and safeguarding of Information Assets in a manner that does not impede the usage of such assets in the Institution's mission of discovery, learning, and engagement.
- May delegate this responsibility to a Data Steward.

Institution Faculty, Staff and Students, and Other Parties with Access to Institution Information Assets and IT Resources

- In accordance with the Institution Statement of Integrity and Code of Conduct, act as stewards of Information Assets and IT Resources.
- Comply with the policies, standards and procedures that support the Information Security and Privacy Policy, including supporting Institution information security activities and applicable compliance programs.

- Complete awareness training as necessary or appropriate to meet Institution information security objectives and to ensure compliance with applicable laws, regulations and Institution policies.

DEFINITIONS

All defined terms are capitalized throughout the document.

Data
Discrete, objective facts, statistics or other information collected or captured for reference, analysis, calculation, measurement or some other use.

Data Steward
An individual assigned by an Information Owner to facilitate the interpretation and implementation of Data policies, standards and procedures.

Data User
An individual who needs and uses Information Assets on a daily basis as part of their assigned employment duties or functions.

Device(s)
Any mechanism used to store, retrieve, manipulate, or transfer Data, including but not limited to, a desktop or laptop computer, CD, USB flash drive, external USB hard drive, tablet, smart phone or cellular phone.

Information Asset
A body of contextualized or definable Data, regardless of format, that has a recognizable and manageable value, risk, content and lifecycle and that is generally defined, classified and managed by the Institution so that it can be understood, shared, protected and used effectively. In the ordinary course of its activities, the Institution regularly creates, collects, maintains, uses and transmits Information Assets.

Information Owner
The unit administrative head who is the decision-maker with respect to Information Assets owned by that unit in conducting Institution business. Except in cases where unit-level control would impede the general usage of information in the Institution's mission of discovery, learning and engagement, an Information Owner has decision-making authority over the Information Assets used, managed or regularly accessed in the unit's administrative functions, as well as over any forms, files, information and records, regardless of format, that relate to such Information Assets.

Information Security Governance Committee
A committee of individuals who, due to the nature of their positions within the Institution, have responsibility for oversight of an Information Asset that is subject to compliance with state or federal laws and regulations and/or contractual obligations related to information security and privacy.

IT Resources (or Information Technology Resources)
All tangible and intangible computing and network assets provided by the Institution or by authorized third-parties, regardless of whether those resources or assets are accessed from on-campus or off-campus locations or via Devices. Examples of such assets include, but are not limited to, hardware, software, wired and wireless network and voice telecommunications assets and related bandwidth, mobile Devices, electronic and hardcopy information resources, and printers.