Information Technology

End User Policy

Version: 1.0 Date: 03/02/2021

Policy Title: End User Policy

Policy Type: New policy

Applicability: College-wide

Submitted By: Don Schattle/Dylan Bukaweski, Information Security Office (infosec@providence.edu)

Oversight Department(s): Information Technology

Effective Date: 04/06/2021

1. Policy Statement

The Providence College Information Security Office (ISO) is responsible for taking steps to safeguard the confidentiality, integrity, and availability of information technology (IT) resources and data owned and maintained by the College. In pursuit of this objective, the ISO has established various control practices, many of which are technical in nature and do not involve active participation from individual end users. However, many threat vectors and risks in the modern information security landscape involve the deception and manipulation of end users rather than the exploitation of technologies alone. As such, it is imperative that end users are aware of the duties they must fulfill in order to reduce the likelihood of a breach event or other information security incident.

Ultimately, effective security is a community-wide effort involving the support and participation of all Providence College students, faculty, staff and affiliates who interact with information technology resources. Members of the Providence College community are expected to become familiar with this End User Policy, to act with careful consideration of its requirements, and to seek assistance whenever necessary.

2. Purpose

The purpose of this Policy is to formally establish the responsibilities that end users are expected to fulfill in support of Providence College's information security objectives.

3. Scope

This Policy applies to all students, faculty, staff and agents of Providence College, including all personnel affiliated with third parties. Additionally, this policy applies to all IT resources owned, leased, or otherwise managed by Providence College, as well as all College data – information that is created, stored, processed and/or transmitted in the course of College operations, within or on behalf of any office or department.

4. Policy

4a. Physical and Environmental Security

- Be suspicious of unknown individuals attempting to gain access to sensitive areas within facilities such as data centers, networking closets, safes, vaults, locked filing cabinets, etc. Report such activities immediately to the Office of Public Safety.

- Do not hold doors that are secured via keycard/badge access or similar means open for unfamiliar individuals. This includes individuals claiming to represent third parties hired by Providence College (e.g., vendors, contractors, maintenance personnel). Consult departmental management, the Office of Public Safety, the IT help desk, or the College's Information Security Office if unsure about the legitimacy of a third party requesting physical access to secure location.
- Never tamper with a physical access control device (e.g., keycard/badge reader), surveillance camera, or other physical security equipment.

4b. IT Backup and Recovery

- Utilize only approved storage locations for electronic data/documents such as: departmental network drives and OneDrive. Generally speaking, endpoints are not approved storage locations for College data, especially data that is non-public in nature (e.g., desktops, laptops, mobile devices).
- Be aware that documents, files, and other data stored locally on endpoints are not included in IT backups.
- Understand that requests for restoration of backups, including lost or deleted data/documents, are handled by Information Technology on a case-by-case basis. Additionally, it should be known that full restoration of lost or deleted data/documents from backups is not always technically possible.

4c. IT Help Desk and IT Issue Management

- Report IT problems and issues promptly to the IT help desk.
- Respond back to the IT help desk in a timely manner if additional information is requested regarding a reported problem.
- Recognize that the primary function of the IT help desk is to support College-owned technologies, including college-owned endpoints. For personally-owned endpoints, IT help desk personnel may be able to provide support in a limited capacity for network connectivity and email access issues only.

4d. Information Security Training and Awareness

- Complete information security awareness training upon initial hire and again annually thereafter.
- Acknowledge acceptance of documented information security policies upon initial hire and again annually thereafter.
- Read and understand periodic information security reminder communications distributed via email and other means.

4e. Logical Access Accounts & Activity Logging

- Understand that each user is solely responsible for all activities associated with their user ID.
- End users should be aware that audit trails of activity are generated to support monitoring of IT resources in accordance with the College's information security program.

- Shared user IDs, logins and accounts are prohibited unless explicitly approved by Information Technology.
- Ensure that personnel actions – including new hires, terminations, and job changes – are documented through appropriate channels.

4f. Password and Authenticator Management

- Always safeguard authentication information (e.g., passwords, PINs) for all accounts utilized to access Providence College information systems.
- Never share or disclose authentication information, and be suspicious of anyone asking you to do so via any communication method (e.g., email, phone call, in person). IT staff will never request that you provide your password, especially for technical troubleshooting purposes.
- Always change the initial password provided for a newly provisioned account.
- When prompted or instructed to change a password, do not reuse previous passwords.
- End users should immediately change their password if they suspect that their account has been compromised.
- Passwords must meet enforced length and complexity requirements.
- End users should avoid using passwords that are known to be weak (e.g., “password”, “password123”) or are based on personal information that can be easily researched (e.g., last name, birthday, addresses).

4g. Remote Access Management

- Remote access (e.g., via Virtual Private Network (VPN)) to College information technology resources requires formal approval. The general expectation is that faculty and staff will perform their job duties from their on-campus work location during business hours.
- Remote users will be required to re-authenticate remote access sessions after a period of time.
- Multifactor Authentication (MFA) is required for all remote access to Providence College information technology resources.
- Remote access approvals will be subject to an annual recertification process to validate that a legitimate need for the continuation of access exists.

4h. IT Endpoint Management

- End users are prohibited from attempting to disable or alter endpoint security mechanisms (e.g., anti-virus, host-based firewall) on College-owned endpoints.
- All College-owned devices must be returned upon termination of employment, planned or unplanned.
- Loss or theft of College-owned endpoints must be reported immediately to the Office of Public Safety.

4i. Mobile, BYOD, and Oher Personally-Owned Endpoints

- Minimum security controls must be in place on personally-owned endpoints in order to access College information technology resources. Examples of such controls include, but are not limited to: anti-virus, operating system patches, local system firewall, and a password protected login.
- Providence College IT reserves the right to revoke network access from personally-owned endpoints that have not been configured with minimum security controls.
- Mobile, BYOD and other personally-owned endpoints are generally not approved storage locations for College data, especially data that is non-public in nature.
- Loss or theft of personally-owned endpoints used to access College information systems must be reported immediately to the Office of Public Safety.

4j. IT Third-Party Management

- Established purchasing protocols for procurement of technology and/or IT services must be followed in all cases by all departments.
  - "Technology" is embedded in the vast majority of modern devices. Any equipment with an "on/off" switch or button that will be connected to the College's network must be approved by IT prior to procurement.
  - "IT services" include any internet/cloud technologies that will receive, store, process, and/or transmit College data.
- IT may not be able to implement, support, and maintain technologies or IT services that are procured outside of established protocols.
- Procurement of technologies or IT services outside of established protocols may constitute a violation of the College's information security program. Such technologies may be immediately disconnected from College networks and IT services suspended until minimum required security controls are verified to be in place.

5. Procedure for Reporting an Alleged Violation of the End User Policy

Suspected violations of this Information Technology End User Policy are to be reported in a timely fashion, in writing, to the College's Information Security Office. Email may be sent to infosec@providence.edu. In order to help ensure the fairness of any subsequent investigation, the individual filing the report should not discuss with or provide copies of the report to other persons. Nothing in this reporting procedure shall be interpreted to prohibit an individual from pursuing such other administrative or legal rights as he or she may have and deem necessary.

6. Enforcement

When presented with evidence of a violation of College policies, or state or federal laws, or when it is necessary to do so to protect the College against potential legal liability, the College may suspend, block, or restrict the use of its information technology resources. Violators also may be subject to other penalties and disciplinary action up to and including suspension, dismissal, or termination.

Appendix A – Definition of Terms

- **END USERS**: all personnel that access Providence College **INFORMATION TECHNOLOGY (IT) RESOURCES** as defined in the Acceptable Use Policy:
    a. **HARDWARE**: desktops, laptops, mobile devices, personally owned devices, etc.
    b. **INFORMATION SYSTEMS**: email, Banner, SAKAI, Office365, etc.
    c. **NETWORKS**: campus wired and wireless networks, other networks utilized to access College information technology resources.
    d. **COLLEGE DATA**: information created, received, stored, processed and/or transmitted by the College in the course of operations; vital College assets.
- **ENDPOINTS**: desktops, laptops, tablets, mobile devices, etc. Technologies utilized by the end users to access Providence College information technology resources.
- **COLLEGE-OWNED ENDPOINTS**: devices acquired, owned and managed by Providence College, may be issued to a specific individual, but may also be shared by multiple individuals within a department, for example.
- **PERSONALLY-OWNED or BYOD (Bring Your Own Device) ENDPOINTS**: devices acquired, owned and managed by individuals that may be used to access College information technology resources.
- **MULTIFACTOR AUTHENTICATION (MFA)**: requires using “something you know”, for example: a password, in combination with “something you have”, for example: an access token. Note that an access token can be “hard” – a physical device – or “soft” – a code delivered via SMS to your mobile phone.

Appendix B – Related Policies

- **Information Technology Acceptable Use Policy**
- **Information Technology Resources Privacy Policy**