Carson-Newman Information Security Policy

1. Overview

The Information Security Policy is a set of guidelines dealing with related aspects of the security of the Information Technology Systems at Carson-Newman. It is designed to protect Carson-Newman's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Carson-Newman employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline several security-related practices that are required for use of computer equipment and systems at Carson-Newman. These rules are in place to protect the employee and Carson-Newman. Inappropriate use exposes Carson-Newman to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Carson-Newman business or interact with internal networks and business systems, whether owned or leased by Carson-Newman, the employee, or a third party. All employees, contractors, consultants, temporaries, and other workers at Carson-Newman and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Carson-Newman policies and standards and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Carson-Newman and its subsidiaries and affiliated companies, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Carson-Newman or its subsidiaries or affiliated companies.

4. Policy

4.1 Access Control

4.1.1 Electronic access to Carson-Newman software applications and data storage will be controlled by individual login accounts. This includes both Active Directory authentication as well as individual system logins. The sharing of login information to any system is strictly prohibited.

4.1.2 The level of access any employee has to a given system will follow the Principle of Least Privilege. Specific rights will be requested by the employee’s supervisor. Senior Management and/or the IT Department reserve the right to grant or restrict access as well when needed.

4.1.3 Requests for changes to access must be submitted in writing (email is acceptable) to the IT Department. The IT Department will document all requests and subsequent denials or changes in an electronic ticket system for record keeping purposes.

4.1.4 It is the responsibility of the individual manager to notify the IT Department when an employee has been terminated or when their access is otherwise revoked. IT will disable individual Active Directory login accounts and email access immediately upon receipt of notification. Email accounts may be left open for up to an additional 90 days at the request of Management where business needs require it. In those instances, the password must be changed and access to the temporary mailbox will be granted to the individual(s) designated by Management in the request.

4.5.1 Guest accounts for access to the wireless network may be requested if the user will be active on campus for more than seven days. Any guests that are on campus for less than seven days will be required to fill out the guest account request form every 24 hours.

4.2 Equipment Security

4.2.1 All company owned desktops, laptops, and servers will be protected by an IT Department approved solution. This solution will be installed by IT before any new hardware is deployed for use anywhere in the organization.

4.2.2 Distributed systems will receive updates from an IT-managed server or service. It is the responsibility of the employee to make sure their hardware is connected to the company network at least once every 30 days to receive updates.

4.2.3 Non-approved software must not be installed on any company system.

4.2.4 Disabling, removing, or otherwise tampering with the effectiveness of the corporate solutions is strictly prohibited.

4.2.5 Any personal device that connects to the corporate network must be password protected and protected by a valid and updated antivirus solution. Devices must not be running an operating system more than two releases old.

4.3 Physical Access

The nature of our business requires us to open many of our physical locations up to members, guests, and even the public. Accordingly, we must ensure that we are vigilant in ensuring that physical access to our servers and networks remain restricted.

4.3.1 Main Campus – Physical access to the Server Rooms is controlled behind main front entrances and secondary keyed locks on the server room doors. In our main server location, camera and key card entry are also deployed. Network equipment is stored in nonpublic closets whenever possible.

4.3.2 Remote Locations – Physical access in remote locations is limited by key access or guard service. The main network and server rack(s) are behind locked door. Only the IT Department and select members of management will have this key. Whenever physically possible, the rack(s) must also be located behind a locked door.

4.4 Passwords

4.4.1 Authorized users must keep passwords secure and not share user accounts, personal identification numbers, security tokens, smartcards or similar devices used for identification and authorization purposes. Users are responsible for the security of their passwords and accounts. Users shall not divulge any remote connection sites or access points to the Company's computer resources to anyone without authorization from Information Services.

4.4.2 Network (Active Directory) Passwords are assigned by the IT Department when an account is created using the last 6 digits of the SSN. Users may change their passwords at any time. Student and Employee passwords are set to expire on a scheduled basis.

4.4.3 All other software applications including web-based applications or services are governed by the password policies created by the individual vendors. At a minimum they must require an alpha-numeric password of at least eight characters in length.

4.4.4 Passwords must never be shared among employees, guests, or visitors. Anyone needing access to a system, even on a temporary basis, must go through the process established in section 4.1 of this same policy. The only exception to this will be the password to the guest Wi-Fi access at any location.

4.4.5 If at any time a user suspects their password may have been compromised, it is the user's responsibility to change that password immediately. If assistance is needed with changing any password, users may contact the IT Department for guidance. Active Directory passwords will be changed by the IT Department when requested.

4.5 Security Breaches

4.5.1 If any individual who suspects that a theft, breach, or exposure of protected, sensitive, or personally identifiable data has occurred, they must immediately report it to the IT department. IT will investigate all reported thefts, data breaches, and exposures to confirm if a theft, breach, or exposure has occurred.

4.5.2 If a theft, breach, or exposure has occurred, the CIO along with any other appropriate university leadership will follow current best practices at the time of the incident. This may or may not include:

i. Working with Carson-Newman communications, legal, and/or human resources departments to decide how to communicate the breach to a. internal employees, b. the public, and c. those directly affected.

ii. Contacting forensic investigators and experts to determine how the breach or exposure occurred, the data involved, the scope of impact, and/or determine the root cause.

iii. Contacting the Department of Education if student information was affected.

The IT Department will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by the IT Department team in advance.

5. Enforcement

Any employee found to be in violation of this Policy may be subject to disciplinary action, up to and including termination of employment. Additionally, individuals may be subject to loss of systems access, civil prosecution, and criminal prosecution. Access to computer resources may be suspended immediately upon the discovery of a violation of this policy.

6. Policy Review

The IT Department will review this policy and notate said review in the Revision History section.

7. Revision History

Date of Change	Responsible	Summary of Change
07/29/2022	**David Tuell, CIO**	**Design and information updates**