# Palau Community College
# CYBER SECURITY POLICY

## 1 PURPOSE OF CYBER SECURITY POLICY

Cyber Security Policy is a formal set of rules by which those people who are given access to Palau Community College (PCC) technology and information assets must abide.

The Cyber Security Policy's main purpose is to inform college users (employees, contractors, and other authorized users) of their obligatory requirements for protecting the technology and information assets of the college. It describes the technology and information assets that the college must protect and identifies many of the threats to those assets. It also describes common security threats and user responsibilities for accessing secured and controlled Internet services.

## 2 WHAT THE COLLEGE IS PROTECTING

It is the obligation of all users of the college to protect the technology and information assets of the college. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the college are made up of the following components:

- Computer hardware, CPU, discs, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments and divisions within the college. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

## 3 CLASSIFICATION OF INFORMATION

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The college shall classify the information controlled by them. The college department/division heads are required to review and approve the classification of the information they control and determine the appropriate level of security to best protect it. Administrators must be responsible for maintaining the integrity of computer systems and data held on them and for ensuring the systems are not misused. The college and administrators will identify who should have access to the computer systems and data held on them.

### 3.1 Data Classification System:

**Public** – Information that may or must be open to the general public. It is non-confidential. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Examples include:

Publicly posted web site
Publicly posted job announcements

**Internal** – Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. It is also confidential. This classification applies even though there may not be a civil statute requiring this protection. Internal data is information that is restricted to personnel who have a legitimate reason to access it. Examples include:

General employment data (e.g., excluded SSN, salary)
Contracts

**Confidential** – Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by a specific college personnel (administrator or other designated college personnel) is required for access because of legal, contractual, privacy, or other constraints. Confidential data has a very high level of sensitivity. Examples include:

Social Security Number
Student ID number (if it is the same as the Social Security Number)
Credit card number
Personal identity information (PII)

## 4 THREATS TO SECURITY

In computer security, a threat is a possible danger that might exploit a vulnerability of breach security and therefore cause possible harm. A threat can be ether intentional, accidental, or otherwise a circumstance, capability, action, or event. There are different kinds of security threats, both internal and external, including the following common ones:

### 4.1 Employees

One of the biggest security threats are employees. This is mitigated by the following being done:

- ✓ Authorizing rights to systems for appropriate users
- ✓ Discouraging sharing of accounts and login information unless authorized
- ✓ Removing or limiting access to systems when employees are separated or disciplined

- ✓ Physically securing computer assets, so that only staff with appropriate need can access
- ✓ Ensuring the Technology Resource Use Agreement is understood and followed

## 4.2 Amateur Hackers and Vandals

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses or Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target.

This is mitigated by the following being done:

- ✓ Installing up-to-date security programs, including antivirus, anti-malware software, or anti-spyware
- ✓ Subscribing the college to updated Network Firewalls (every three years)
- ✓ Encouraging employees and students to logout from any site when not in use
- ✓ Considering hosting options for commonly accessed internal services (ex. Web & email service)
- ✓ Educating employees and students not to click on links, open emails and files or run programs that they did not expect to receive
- ✓ Assisting employees to update their OS and other software frequently

## 4.3 Criminal Hackers and Saboteurs

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

This is mitigated by the following being done:

- ✓ Encouraging employees and students to create strong passwords
- ✓ Keeping web application firewalls and anti-virus and other software updated
- ✓ Limiting access at the administrator level

# 5 USER RESPONSIBILITIES

This section establishes usage policy for the computer systems, networks and information resources of the college. It pertains to all employees, students, and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the college.

All users are expected to have knowledge of these security policies and are required to report violations to the Computer Services Office where the Computer Service Director will take appropriate action.

## 5.1 Technology Resource Use Agreement

All students and employees must agree to and sign the Technology Resource Use Agreement. All students must agree to the Student Wi-Fi User Agreement upon connecting to the Student Wi-Fi.

# 6 ACCESS CONTROL

A fundamental component of the College's Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

## 6.1 User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with any other employee whatsoever. All users should comply with the following rules regarding the creation and maintenance of passwords:

- ✓ Avoid words that can be found in an English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools". Instead, passwords should be at least 8 characters long and should be a combination of uppercase and lowercase letters, numbers and symbols.

- ✓ Passwords should not be posted on or near computer monitors or towers or otherwise be readily accessible in the area around the computer.

- ✓ It is strongly recommended that passwords be changed every 6-12 months or as necessary.

- ✓ User accounts will be frozen after 5 failed logon attempts.

- ✓ Logon IDs and passwords will be suspended after 30 days without use, except for those systems being used once a semester.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to log on as a System Administrator. Users who need this level of access to production systems must request a Special Access account.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, or otherwise leaves the employment of the college. Student accounts will be deleted each semester.

Supervisors / Managers shall immediately and directly contact the college Human Resource office personnel to report change in employee status that requires terminating or modifying employee logon access privileges. The Human Resource office will inform the computer service personnel to take appropriate action.

Employees who forget their passwords must call the Computer Service office to get new passwords assigned to their accounts. The employee must identify himself/herself to the Computer Service office.

## 6.2 System Administrator Access

System Administrators, network administrators, and security administrators will have full access rights to host systems, routers, hubs, and firewalls as required to fulfill the duties of their jobs.

All system administrator passwords will be changed immediately after any employee who has access to such passwords is terminated, fired, suspended, or otherwise leaves the employment of the college.

## 6.3 Special Access

Special access accounts are provided to individuals requiring temporary or permanent system administrator privileges in order to perform their jobs. These accounts are monitored by the college and require the permission of the college department/division heads. Special accounts may expire or be renewed as directed by department and/or division heads.

## 6.4 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between PCC and all third-party companies and other entities required to electronically exchange information with the college. When third –party entities need to be connected, the appropriate personnel will notify the Computer Services Office for connection and the third-party entity must sign the Technology Resource Use Agreement.

“Third-party” refers to vendors, consultants and business partners doing business with the college, and other partners that have a need to exchange information with the college. Third-party network connections are to be used only by the employees of the third-party, only for the

business purposes of the college. The third-party company will ensure that only authorized users will be allowed to access information on the college network. The third-party will not allow Internet traffic or other private network traffic to flow into the network. A network connection will terminate right after the third-party has completed its business with college.

This policy applies to all third-party connection requests and any existing third-party connections.

## 6.5 Connecting Devices to the Network

Only authorized devices may be connected to the College network(s). Authorized devices include PCs and workstations owned by the college that comply with the configuration guidelines of the college. Other authorized devices include network infrastructure devices used for network management and monitoring. Connection to the network will be completed by the Computer Service office personnel.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

## 6.6 Remote Access

Only authorized persons may remotely access the college's systems. Remote access is provided to those employees, contractors and business partners of the college that have a legitimate business need to exchange information, copy files or programs, or access computer applications. The authorized connection can be remote PC to the network or a remote network to the college network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID assigned by the college Computer Services.

## 6.7 Unauthorized Remote Access

The attachment of any devices (e.g. hubs) to a user's PC or workstation that is connected to the college LAN is not allowed without college permission. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

# 7 PENALTY FOR SECURITY VIOLATION

The college takes the issue of security seriously. Those individuals who use the technology and information resources of the college must be aware that they can be disciplined if they violate this policy. **Upon violation of this policy, an employee of the college may be subject to disciplinary procedures as stated in the Technology Resource Use Agreement.**

In a case where the accused person is not an employee of the college, the matter shall be submitted to the appropriate college personnel. The appropriate college personnel may refer

the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

# 8 SECURITY INCIDENT HANDLING PROCEDURES

This section provides some policy guidelines and procedures for handling security incidents. The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the college network.

Some examples of security incidents are:

- Illegal access of a college computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a college computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a college web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against another computer outside of the college network. For example, the computer service office notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees who believe their computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used should report the situation to Computer Service immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.