BAY de NOC COMMUNITY COLLEGE BOARD OF TRUSTEES POLICIES

1000 GENERAL ADMINISTRATION

1050 INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY

It shall be the policy of the Bay de Noc Community College Board of Trustees, that Bay College maintain security of its Information Technology infrastructure. Bay College collects and maintains sensitive data relating to its students, employees, and individuals associated with Bay College, and is dedicated to ensuring privacy and proper handling of this sensitive data, under all state and federal data privacy laws. This Policy provides the framework for protection of this sensitive data and Bay College's Information Technology infrastructure and outlines protocols that govern data and cybersecurity measures, and defines training requirements along with the disciplinary process for policy violations. This Policy applies to all Bay College employees (full-time, part-time, permanent, and temporary), students, remote workers, contractors, volunteers, interns, Bay College partners, and/or any individuals with access to Bay College's electronic systems, information, software, and/or hardware (hereinafter referred to as Users).

Bay College may monitor any Internet or Information Technology resource activity on Bay College equipment or within Bay College accounts. Discovery of activities which do not comply with applicable law or policy may result in discipline.

Bay College assumes no liability for any direct or indirect damages arising from the Users connection to the Internet. Bay College is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material they access and disseminate through the Internet.

PROCEDURE:

1050.1 Definitions

a. Sensitive Data

- Items covered by the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability Accountability Act (HIPAA), and Payment Card Industry Data Security Standards (PCI DSS);
- Third-party Confidential Information (both sent and received);
- Personally Identifiable Information (PII);
- Financial information when integrity, confidentiality, and/or availability are an issue;
- Information subject to the Attorney-Client Privilege;

- Information with a defined records retention and disposal schedule;
- Safety/security information;
- Building technical specifications;
- Misconduct information; and
- Title IX information and case details.

b. Data Owner
A department or position responsible for the accuracy and integrity of data elements within the larger context of the College's Information Technology infrastructure.

c. Encryption
The process of converting information or data into a code, especially to prevent unauthorized access.

d. Gaming
The action or practice of playing video games.

e. Peer-to-Peer File Sharing
Denoting or relating to computer networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server.

f. Maxient
The College uses a system called Maxient to manage cases associated with misconduct, policy violations, and safety/security.

g. RT (Request Tracker)
The system used to track requests for access to sensitive data. This system tracks both the request and the granting and serves as the audit trail.

1050.2 Sensitive Data Security

Bay College will protect the confidentiality, integrity, and availability of sensitive data accessed, managed, and/or controlled by Bay College, including electronically stored data, printed materials, and verbally communicated information. Users entering sensitive data into the College's systems must do so with integrity and accuracy to ensure the highest quality. Integrity and accuracy of sensitive data is critical across all information

systems including electronically stored data, printed materials, and the spoken word.

All users with access to sensitive data sign a confidentiality agreement at the time of hire or when access is requested and granted. Requests and subsequent granting of access is recorded through RT. Sensitive data access requires explicit permission from the data owner. All applicable regulations associated with the sensitive data will be passed on to the User granted access through training.

a. Training related to sensitive data security is a shared responsibility between the Supervisor and the employee (or User).

   Supervisor Responsibilities:

   - Arrange training on applicable software platforms and inform Users about applicable policies when requesting access to the information systems.
   - Coordinate with IT and the Data Standards Committee to define controls and processes within their department to ensure data accuracy and consistency with data standards.
   - Address data entry errors with Users and take proper action to ensure mandatory training.
   - Verify proper testing by employee (or Users) before and after upgrades performed on information systems.
   - Verify documentation on data and processes are available upon request.

   Employee (or User) Responsibilities:

   - Understand processes and data standards and take proper care to ensure quality and accuracy of data being entered.
   - Ensure processes involving data are thoroughly documented, including the schedule on which the process is to occur.

- Take prompt corrective action when a problem with data entry is identified.

- Perform duplicate data searches before entering data into an information system.

- Verify data entry procedures and processes in test environments before and after system upgrades occur.

b. When access to sensitive data is granted, the least access required to perform job functions based upon role and responsibility will be provisioned.

c. Encryption is required whenever transmitting or storing sensitive data.

d. Physical security measures must be in place to restrict access to printed materials or electronic systems that store sensitive data.

e. Notify law enforcement and IT when a device containing sensitive data has been stolen or is missing.

1050.3 Social Security or International Number Privacy

Bay College, through procedures implemented and promulgated by Administration, will ensure, to the extent practicable, the confidentiality of Social Security and International numbers collected and maintained through the necessary course of conducting college business. Social Security and International numbers will only be obtained from individuals for legitimate business reasons or when required by law.

a. Bay College prohibits unlawful or unnecessary disclosure of Social Security and International numbers and requires its Users to properly protect and secure this information, whether in electronic or physical form.

b. Only Users who have legitimate reasons may access information or documents that contain Social Security or International numbers. Administration is responsible for designating specific Users who may access Social Security and International numbers.

c. Social Security and International numbers must be disposed of so it protects confidentiality.

1050.4 Internet and IT Resources Acceptable Use

IT resources are to be used exclusively for Bay College related activities in alignment with the College's mission. Bay College may monitor any Internet or IT resource activity on Bay College equipment or within Bay College accounts.

a. Appropriate Use
   - To complete job duties and/or provide academic resources.
   - To improve upon work or academic resources.

b. Inappropriate Use
   - Used for illegal or unlawful purposes, including, but not limited to, copyright infringement, viewing obscene, pornographic, or illegal images or materials, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, illegal impersonation, illegal gambling, soliciting for illegal pyramid schemes, computer tampering (*e.g.* spreading computer viruses).

   - Used in any way that violates Bay College's policies, rules, or administrative orders.

   - Users may not join Bay College computers to any peer-to-peer network without prior approval from IT.

c. Gaming
   - Gaming on Bay College owned equipment is permitted in designated locations as determined by IT during established periods of time that do not interrupt academic activity.

   - Game installation and updating is coordinated with IT.

   - Tournaments and club related activities are coordinated with the Director of Student Life.

   - Equipment used for gaming activities is to be restored to previous setup when gaming event is complete.

1050.5 Passwords and Accounts

a. Passwords are constructed according to set length and complexity requirements. Passwords are at least 8 characters in length and include a mix of letters and numbers, include at least one special character, and can

be no combination of a User's given name or their Bay College userid. These requirements are subject to change without notice.

b. Passwords have a lifespan and are changed at minimum once every 365 days and previous passwords cannot be reused more frequently than every 6 changes.

c. Passwords shall be used and stored in a secure manner. Passwords are not to be written down or stored electronically in plain text but can be stored electronically utilizing the customary encryption protocols of the time.

d. Users will take care to obscure password entry into login screens and passwords must be transmitted in an encrypted format.

e. Account and password information is assigned individually and cannot be shared with any other person. Attempting to obtain or use another person's account information is strictly prohibited. Users must take all necessary precautions to prevent unauthorized access to their account(s).

1050.6 Peer-to-Peer File Sharing

Bay College will comply with Federal Law – H.R. 4137, Higher Education Opportunity Act (HEOA) and make an annual disclosure informing students and employees that illegal distribution of copyrighted materials, including unauthorized peer-to-peer file sharing, may lead to civil and/or criminal penalties.

a. IT will monitor for illegal distribution of copyrighted materials, including unauthorized peer-to-peer file sharing.

b. Bay College will remind Users of this law annually during the fall semester. The law will also be referenced in the student handbook.

c. Alternatives to illegal file sharing will be provided to Users when requested. For more information on legal alternatives, visit RIAA https://www.riaa.com/resources-learning/for-students-educators/ and MPAA https://www.mpaa.org/what-we-do/fostering-innovation/#where-to-watch.

1050.7 Remote Access/Remote Work

Remote access and remote work mean a User connects to Bay College IT resources, that are not public facing, through a secure connection. All remote access and mobile privileges for Bay College Users to access Bay College resources – and for wireless Internet access via hotspots – must use Bay College approved methods. *Connecting to public facing Bay College resources such as Bay College website or myBay are not considered remote access and are not governed by this policy.*

Remote access is defined as any connection to Bay College's network or other IT resources from off-site (not on a Bay College campus), such as the User's home, a hotel room, airports, cafés, satellite office, wireless devices, etc.

a. All remote access will be centrally managed by Bay College's IT Department and will utilize encryption and strong authentication measures. Remote access connections covered by this policy include but are not limited to VPN, SSH, direct dial cable modems, remote desktop connections, and proprietary remote access/control software supplied by IT.

b. It is the responsibility of the User who has remote access privileges to ensure their remote access connection remains secure. All remote access connection activities are to be used appropriately, responsibly, and ethically. Therefore, these rules must be observed:

   - General access to the Internet by residential remote Users through Bay College's network is permitted. However, the User shall not use Bay College's network to access the Internet for recreational purposes.

   - All remote computer equipment and devices used for Bay College activities will have reasonable physical security measures and antivirus software approved by the IT Department.

   - Users must connect to the Bay College VPN before accessing Remote Resources.

   - Users cannot modify remote access connection settings without prior written communication with Bay College IT. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

- All remote access connections shall include a *time-out* system. In accordance with Bay College's security policies, remote access sessions will time out after 120 minutes of inactivity and shall terminate after 8 hours of continuous connection.

- If any computer or related equipment, including personal equipment, used for remote access is damaged, lost, or stolen, the User must promptly notify Bay College's IT Department and their Supervisor.

- The User shall immediately report any incident or suspected incidents of unauthorized access and/or disclosure of college resources, databases, networks, etc.
- The User agrees to and accepts that their access and/or connection to Bay College's network(s) may be monitored to identify unusual patterns or other suspicious activity.

1050.8 Use of Personal Equipment and Accounts for Bay College Activities

Any record created by a User related to Bay College activities (including text messages, voicemails, emails, and any other electronic communication) are considered a college record. These records are to be maintained in compliance with regulations, retention policies, and may be subject to Freedom of Information Act (FOIA) disclosure requests.

a. Personal text messaging, personal email, and personal voicemail are to be used for general communication only. This communication does not require retention. Users must delete general communication text messages as soon as the conversation is complete.

b. No sensitive college data may exist on personal equipment or accounts.

c. If a User receives information on a personal device that requires record retention, the User must transfer the information to a college file server or college email.

d. Bay College owned and/or personal devices used for any Bay College activities must be protected with a PIN or auto-lock to prevent unauthorized access.

1050.9 Cloud Services

Bay College utilizes online, hosted (cloud-based) storage and collaboration services. Sensitive, proprietary, and/or confidential data shall not reside on

cloud services unless Bay College has entered into a legal contract with the service provider or Bay College owns and operates the system. Contracts are approved by the Vice President of Finance and Operations.

a. Cloud services may not be used for sensitive data.

b. Any Bay College data residing within a cloud service must be retrievable by the College. The individual who manages the data is expected to coordinate with the IT Department to ensure Bay College can access data within the cloud service.

c. Data stored within cloud services must follow applicable records retention and disposal schedule(s).

d. All cloud services will be screened before entering into a contract. Screening will include backups, disaster plan, data security, and encryption standards. Before a contract is signed, Bay College will develop an exit strategy with steps to recover college data from the provider.

1050.10 Discipline

Bay College disciplinary protocols are based on the severity of the violation. All violations of this Policy will be recorded in Maxient. Each case will detail the policy section impact, the cause of the violation, previous trainings, and any previous violations and disciplinary actions of this Policy if applicable. Violations of this Policy may result in mandatory training and/or temporary or permanent revocation of access to some or all computing and networking resources and facilities; disciplinary action according to applicable Bay College policies; and/or legal action according to state and federal laws and contractual agreements.