Reviewed by the Standards & Finance Committee in November 2021
Approved by Corporation in December 2021
Next review due: 3 years November 2024

Brockenhurst College

INFORMATION SECURITY POLICY

1. Introduction

To safeguard Brockenhurst College's information technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Security Policy reflects Brockenhurst College's commitment to comply with required standards governing the security of sensitive and confidential information.

Brockenhurst College can minimize inappropriate exposures of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as Payment Card Industry Data Security Standard – "PCI DSS"), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses Brockenhurst College's information technology resources. It is the responsibility of employees, contractors, business partners, and agents of Brockenhurst College. Each should become familiar with this policy's provisions and the importance of adhering to it when using Brockenhurst College's computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the Information Technology Department.

2. Purpose / Scope

The purpose of this security policy is to establish rules to ensure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of Brockenhurst College's information technology resources. The policy assigns responsibility and provides guidelines to protect Brockenhurst College's systems and data against misuse and/or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorised to connect to Brockenhurst College's data network. It may apply to users of information services operated or administered by Brockenhurst College (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with Brockenhurst College are subject to these same definitions and rules when they are using Brockenhurst College's information technology resources.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorised destruction, disclosure or modification of hardware, software, networks and/or data.

This security policy has been written to specifically address the security of data used by the Payment Card Industry. Credit card data stored, processed or transmitted by Brockenhurst College must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

Sensitive credit card data is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

3. Security Policy Ownership and Responsibilities

It is the responsibility of the Senior Management Team (SMT) to publish and disseminate these policies to all relevant Brockenhurst College system users (including vendors, contractors, and business partners). Also, the SMT must see that the security policy addresses and complies with all standards Brockenhurst College is required to follow (such as the PCI DSS). This policy document will also be reviewed annually by the College (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the Vice Principal – Director of Finance

4. Protect Sensitive Data

Sensitive and/or confidential data (e.g., Cardholder Data) must be protected when stored and when it is in transit over public (or untrusted) networks. Strong industry standard encryption methodologies must be used to protect data stored on hard drives, removable media, backups, etc. The following policies ensure proper encryption of stored data and data in transit over open, public networks.

1. Protect Stored Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of sensitive data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable. Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc. The following policies address the treatment of sensitive credit card data. See the document published by the Payment Card Industry Security Standards Council entitled “PCI-DSS Requirements and Security Assessment Procedures v1.2” p. 4 for definitions of cardholder data types.

<u>Storage of Sensitive Credit Card Authentication Data</u>

- Never store sensitive cardholder data such as the authentication data (Track, CVC, PIN) after an authorisation event has taken place (even if encrypted). (PCI-DSS Requirement 3.2)
- Never store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere) in any database, log file, debug file, etc. after any type of card authorisation event. (PCI-DSS Requirement 3.2.1)
- Never store the credit Card Validation Code (CVC) data (3 or 4 digit number located on the back or front of the customer's plastic card) in any database, log file, debug file, etc. after any type of card authorisation event. (PCI-DSS Requirement 3.2.2)
- Never store the cardholders Personal Identification Number (PIN) data (includes actual PIN number or Encrypted PIN block obtained during a debit card transaction from the PIN Entry Device) in any database, log file, debug file, etc. after any type of card authorisation event. (PCI-DSS Requirement 3.2.3)

Mask Credit Card Numbers in Displays Wherever Possible

- Credit card PAN data will be masked or truncated when displaying card numbers on any media (exceptions may be made for those users who have a valid business need to see full PAN data). (PCI-DSS Requirement 3.3)

2. Encrypt Transmissions of Sensitive Data Over Public Networks

- Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Improperly configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to sensitive data environments.

Transmission of Card Data Via End User Messaging Technologies

- Prohibit the transmission of unencrypted cardholder data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (PCI-DSS Requirement 4.2)

Implement Strong Access Control Measures

Access to system components and software within the sensitive data environment (cardholder data network) must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

3. Restrict Access to Sensitive Data by Business Need to Know

Systems and processes must be in place to limit access to critical data and systems based on an individuals need to know and according to job responsibilities.

"Need to know" is when access rights are granted to the least amount of data and privileges needed to perform a job.

Restrict Access to Systems in Cardholder Data Environment

- Access to cardholder data and systems handling cardholder data must be restricted by business need to know. (PCI-DSS Requirement 7.1)

- Automated role based access control systems must be in place on all systems in the cardholder data network. User ID's must limit user's rights to only those necessary for their job classification and function. (PCI-DSS Requirement 7.1.2)

4. Restrict Access to Sensitive Data and System Components

Any physical access to data or systems that house sensitive data (cardholder data) provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

Securing Hard Copy Materials

- Brockenhurst College will define procedures required for protecting paper and hard copy materials (which includes paper receipts, mail, reports, and faxes) containing cardholder data within all facility locations. (PCI-DSS Requirement 9.6)

Secure Media Containing Sensitive Data

- Brockenhurst College will define specific procedures required for controlling the internal or external distribution of any kind of media containing cardholder data. Maintain strict control over the storage and accessibility of both hardcopy and electronic media that contains cardholder data. (PCI-DSS Requirement 9.7, 9.9)

- All forms of media containing cardholder data is required to be classified as sensitive and must be labelled so as to be identified as confidential data. (PCI-DSS Requirement 9.7.1)

- All media containing sensitive cardholder data sent outside the facility must be transferred by secured courier or other delivery method that can be accurately tracked. Log all transfers of media containing cardholder data. Logs must show management approval, and tracking information. Retain media transfer logs. (PCI-DSS Requirement 9.7.2)

- Management approval is required prior to moving any and all media containing cardholder information out of a secured area (especially when media is distributed to individuals). (PCI-DSS Requirement 9.8)

- Periodic inventory of stored media containing cardholder data must be performed and documentation must be retained showing these inventories were performed. (PCI-DSS Requirement 9.9)

Media Destruction Policies

- Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. (PCI-DSS Requirement 9.10)

- Brockenhurst College must define and document specific procedures that will be used to destroy any hard copy materials containing cardholder data beyond reconstruction. Technologies such as shredding, incineration, pulping, etc. must be used to destroy media. (PCI-DSS Requirement 9.10.1)

Maintain an Information Security Policy

Without strong security policies and procedures many of the layers of security controls become ineffective at preventing data breech. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining the Brockenhurst College security policies described above.

5. Maintain a Security Policy for Employees and Contractors

A strong security policy sets the security tone for Brockenhurst College and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.

“Employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site.

Publish, Distribute, and Update the Information Security Policy

- Brockenhurst College requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI-DSS Requirement 12.1)

- The Brockenhurst College information security policy must be reviewed at least annually to keep it up to date with changes in the industry and with any changes in the cardholder network environment. (PCI-DSS Requirement 12.1.3)

Employee Facing Technologies

- Brockenhurst College must develop usage policies for all critical employee-facing technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage). (PCI-DSS Requirement 12.3)
- Usage of employee facing technologies (see above) requires explicit approval by authorised parties. (PCI-DSS Requirement 12.3.1)
- A list of all devices and personnel with access to these technologies must be kept. (PCI-DSS Requirement 12.3.3)
- Explicitly define all acceptable use of employee facing technologies. (PCI-DSS Requirement 12.3.5)

Please refer to the Brockenhurst College IT & Telecommunications Systems Regulations, Policies and Procedures Handbook.

Assign Information Security Responsibilities & Train Employees

- The Brockenhurst College's information security policy and procedures must clearly define the information security responsibilities of both employees and contractors. (PCI-DSS Requirement 12.4)
- Responsibilities of information security at Brockenhurst College must be formally assigned to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5) Specifically the following responsibilities must be assigned (see form in Appendix A):
  - Responsibility of distributing the Brockenhurst College information security policies and procedures must be formally assigned to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5.1)
  - Responsibility to monitor, analyse, and distribute security alerts and information. (PCI-DSS Requirement 12.5.2)
  - Generate detailed documentation security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5.3)
  - Responsibility to administer users in the cardholder data network. Includes all additions, deletions and modifications to user access. (PCI-DSS Requirement 12.5.4)
  - Responsibility to monitor and control all access to sensitive cardholder data. (PCI- DSS Requirement 12.5.5)
- A formal security awareness program must exist and participation is required for all employees working within the cardholder data environment. (PCI-DSS Requirement 12.6.1)

Policies for Sharing Data with Service Providers

If cardholder data is shared with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modelling purposes), the following policies and procedures must be followed:

- Brockenhurst College must maintain a documented list of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.1)
- Any written agreement with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, must include an acknowledgement of the service provider's responsibility for securing all cardholder data they receive from Brockenhurst College. (PCI-DSS Requirement 12.8.2)
- Prior to engaging with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, Brockenhurst College will conduct due diligence and follow an established process to ensure that the security of cardholder data within the service providers network has been addressed. (PCI-DSS Requirement 12.8.3)
- Brockenhurst College will have an ongoing program to monitor the PCI DSS compliance status of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.4)

Appendix A – Management Roles and Responsibilities

Assignment of Management Roles and Responsibilities for Security

As required by this security policy, the following table contains the assignment of management roles for security processes.

Management Security Responsibilities

Name of Individual or Group	Description of Responsibility
Senior Management Team	Establish, document, and distribute security policies
Senior Management Team	Monitor, analyse, and distribute security alerts and information
Senior Management Team	Establish, document, and distribute security incident response and escalation policies
IT Services Department	Administration of user accounts on systems in the cardholder data network which are directly managed by the College
IT Services Department	Monitor and control all access to cardholder data on the College's network and subsequent systems

Appendix B – Agreement to Comply

Agreement to Comply with Information Security Policies

All employees working with sensitive cardholder data must submit a signed paper copy of this form. Brockenhurst College management will not accept modifications to the terms and conditions of this agreement.

_____

Employee's Printed Name

_____

Employee's Job Title and Department

I, the user, agree to take all reasonable precautions to assure that Brockenhurst College internal information, or information that has been entrusted to Brockenhurst College by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with Brockenhurst College, I agree to return to Brockenhurst College all information to which I have had access as a result of my position with Brockenhurst College. I understand that I am not authorised to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal Brockenhurst College manager who is the designated information Owner.

I have access to a copy of the Brockenhurst College Information Security Policy and also the IT & Telecommunications Systems Regulations, Policies and Procedures Handbook, which I have read and understood, and I understand how it impacts my job. As a condition of continued employment at Brockenhurst College, I agree to abide by the policy. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from Brockenhurst College, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password. I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognisable way (Please refer to page 8 of the Brockenhurst College IT & Telecommunications Systems Regulations, Policies and Procedures Handbook).

I also agree to promptly report all violations or suspected violations of information security policies to Limor Feingold Vice Principal (Finance).

_____

Employee's Signature