Information Security Policy

Burgess Hill Theatre Club

(Company Name)

16 February 2022

(Date)

Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential club information and must be distributed to all members. All committee members must read this document in its entirety and it must be ratified at committee meeting. This document will be reviewed and updated by committee on an annual basis or when relevant to include newly developed security standards into the policy and distributed to all members as applicable.

2. Information Security Policy

Burgess Hill Theatre Club handles sensitive cardholder information regularly. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.
Burgess Hill Theatre Club commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end the committee is committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.
Club members handling Sensitive cardholder data should ensure:

1. Handle Company and cardholder information in a manner that fits with their sensitivity;
2. Limit personal use of Burgess Hill Theatre Club information and telecommunication systems and ensure it doesn't interfere with performance;
3. Burgess Hill Theatre Club reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment for any purpose;
4. Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
5. Do not disclose membership information unless authorised;
6. Protect sensitive cardholder information;
7. Keep passwords and accounts secure;
8. Request approval from committee prior to establishing any new software or hardware, third party connections, etc.;
9. Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit committee approval;
10. Always leave all areas clear of sensitive cardholder data and lock computer screens when unattended;
11. Information security incidents must be reported, without delay, to the Data Protection Officer.

We each have a responsibility for ensuring our club's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your Data Protection officer.

3. Acceptable Use Policy

The Committee's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Burgess Hill Theatre Club's established culture of openness, trust and integrity. Committee is committed to protecting the members, partners and Burgess Hill Theatre Club from illegal or damaging actions by individuals, either knowingly or unknowingly. Burgess Hill Theatre Club will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- All members are responsible for exercising good judgment regarding the reasonableness of personal use.
- All members should ensure that they have appropriate credentials and are authenticated for the use of technologies
- All members should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Committee members should ensure that technologies should be used and setup in acceptable locations.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by committee members from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Burgess Hill Theatre Club, unless posting is in the course of business duties.
- Committee members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by a member will result in disciplinary action, from warnings or reprimands up to and including termination of membership. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Protect Stored Data

- All sensitive cardholder data stored and handled by Burgess Hill Theatre Club and its members must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by Burgess Hill Theatre Club for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Burgess Hill Theatre Club if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7. Access to the sensitive cardholder data

All Access to sensitive cardholder data should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.

- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to members that have a legitimate need to view such information.
- No other members should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- Burgess Hill Theatre Club will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the cardholder data that the Service Provider possess.
- Burgess Hill Theatre Club will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- Burgess Hill Theatre Club will have a process in place to monitor the PCI DSS compliance status of the Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Members are responsible for exercising good judgment regarding the reasonableness of personal use.
- Members should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Members should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Members should ensure that technologies should be used and setup in acceptable locations
- A list of devices that accept payment card data should be maintained.
    - The list should include make, model and location of the device
    - The list should have the serial number or a unique identifier of the device
    - The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Members using the devices should be trained and aware of handling the POS devices
- Members using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.

- Members using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the Data Protection Officer.
- A “visitor” is defined as a vendor, guest of a member, service personnel, or anyone who needs to enter the premises for a short duration.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, USB sticks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted member when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between members and visitors, especially in areas where cardholder data is accessible. “Member” refers to Burgess Hill Theatre Club members, patrons, temporary members and consultants who are “resident” on Burgess Hill Theatre Club sites. A “visitor” is defined as a vendor, guest of a member, service personnel, or anyone who needs to enter the premises for a short duration.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by committee.
- Strict control is maintained over the storage and accessibility of media
- All computers that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by committee, logged and inventoried before leaving the premises. Only secure

courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Burgess Hill Theatre Club, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- Burgess Hill Theatre Club will destroy hardcopy (paper) materials. All hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- Burgess Hill Theatre Club will destroy electronic media.
  - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
  - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into club practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all committee members and members managing card holder information.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day club practice.
- Distribute this security policy document to all committee members to read. This will be ratified at committee annually (see Appendix A)
- All Officers of the club (Chair, Secretary and Treasurer) will undergo background checks (such as criminal and credit record checks, within the limits of the local law through the Bank Account management process) as they commence their term with Burgess Hill Theatre Club.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

- Company security policies must be reviewed annually and updated as needed.

12. Network security

There is a BT WiFi Network router and access available to Burgess Hill Theatre Club premises only. The WiFi Network is managed by BT and has 2 levels of user access. We provide public access via the BT Public Wifi option but our networks are separate for members of the club and the general public.

13. System and Password Policy

There is no System hosted/managed by the Burgess Hill Theatre Club. All tools used to support the running of the theatre, such as TicketSource, are accessed on multiple devices, are managed outside of the club and we adhere to their strict requirements governing security and passwords.

14. Anti-virus policy

- All POS machines must be configured to run the latest anti-virus software as approved by Burgess Hill Theatre Club in accordance with Barclaycard Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example USB sticks and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- End users must not be able to modify and any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

15. Patch Management Policy

There is a separated Wifi network managed by BT and no systems hosted/managed on the premises.

16. Remote Access policy

There is a separated Wifi network managed by BT and no system with remote access hosted/managed on the premises.

17. Vulnerability Management Policy

All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
There is a WiFi network and no system hosted/managed to Burgess Hill Theatre Club at the premises. Burgess Hill Theatre Club agrees to maintain the Barclaycard point of sale device in accordance with Barclaycard instructions and the club will seek to keep themselves informed with any CVSS rated vulnerabilities that could impact the club.

18. Configuration standards:

There is a separated Wifi network managed by BT and no system hosted/managed on the premises.

19. Change control Process

There is a separated Wifi network managed by BT and no system hosted/managed on the premises. Burgess Hill Theatre Club agrees to maintain the Barclaycard point of sale device in accordance with Barclaycard instructions as it does with all externally hosted tools.

20. Audit and Log review

There is a separated Wifi network managed by BT and no system hosted/managed on the premises. Burgess Hill Theatre Club agrees to maintain the Barclaycard point of sale device in accordance with Barclaycard instructions as it does with all externally hosted tools.

21. Secure Application development

There is a separated Wifi network managed by BT and no system hosted/managed on the premises. Burgess Hill Theatre Club agrees to maintain the Barclaycard point of sale device in accordance with Barclaycard instructions as it does with all externally hosted tools..

22. Penetration testing methodology

There is a separated Wifi network managed by BT and no system hosted/managed on the premises. Burgess Hill Theatre Club agrees to maintain the Barclaycard point of sale device in accordance with Barclaycard instructions as it does with all externally hosted tools..

23. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled member, and their intention might be to steal information or money, or just to damage your club.
The Incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant committee members, and take steps to ensure that they understand it and what is expected of them.
Committee members of Burgess Hill Theatre Club will be expected to report to the Data Protection Officer for any security related issues.

Burgess Hill Theatre Club PCI security incident response plan is as follows:

1. Each member must report an incident to the Data Protection Officer.
2. The Data Protection Officer receiving the report will advise the Committee.
3. The Committee will investigate the incident and limit the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The Committee will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The Committee will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
6. If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Data Protection Officer or Committee member who has the authority to stop, cease, shut down, and remove the offending device immediately.

7. A member that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform Burgess Hill Theatre Club Data Protection Officer. After being notified of a compromise, the Data Protection Office, along with other designated committee members, will implement the PCI Incident Response Plan to assist and augment the response plans.

Burgess Hill Theatre Club PCI Security Incident Response Team: **(Update as applicable)**

Officers of the Burgess Hill Theatre Club
Data Protection Officer

Incident Response Notification

Escalation Members

Escalation – First Level
Data Protection Officer

Escalation – Second Level
Committee

Escalation – Third Level
Officers of the Club

The card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the information Data Protection Officer or Committee Member immediately.
2. The Data Protection Officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Data Protection Officer will alert the committee and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and

the law enforcement.

- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level (High, Medium, Low)
   c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
   a. Include forensic tools used during investigation

V. Findings
   a. Number of accounts at risk, identify those stores and compromised
   b. Type of account information at risk
   c. Identify ALL systems analyzed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)
   e. Timeframe of compromise
   f. Any data exported by intruder
   g. Establish how and source of compromise
   h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
   i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA.

Its unauthorized disclosure could seriously and adversely impact VISA, its committee members, member banks, business partners, and/or the Brand

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Committee members of Burgess Hill Theatre Club will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to the members within Burgess Hill Theatre Club. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
4. Obtain additional specific requirements from Discover Card

American Express Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
   Obtain additional specific requirements from American Express

24. Roles and Responsibilities

- Data Protection Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:
  - Creating and distributing security policies and procedures.
  - Monitoring and analysing security alerts and distributing information to appropriate information security.
  - creating and distributing security incident response and escalation procedures that include:
    - Maintaining a formal security awareness program for all committee members that provide multiple methods of communicating awareness and educating committee members (for example, posters, letters, meetings).

25. Third party access to card holder data

- All third-party companies providing critical services to Burgess Hill Theatre Club must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with Burgess Hill Theatre Club's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:

  1. Adhere to the PCI DSS security requirements.
  2. Acknowledge their responsibility for securing the Card Holder data.
  3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
  4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
  5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

26. User Access Management

- Access to Burgess Hill Theatre Club is controlled through a formal user registration process in accordance with the Third Party tools used.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by committee.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy). The request is free format, but must state:

  Name of person making request:
  Job title of the newcomers and workgroup:
  Start date:
  Services required:
- As soon as an individual leaves Burgess Hill Theatre Club membership, all his/her tooling logons must be immediately revoked.
- As part of the Membership termination process the committee will inform all leavers and their date of leaving.

27. Access Control Policy

- Access Control procedures are in place to protect the interests of all users of Burgess Hill Theatre Club tooling by providing a safe, secure and readily accessible environment in which to work.
- Burgess Hill Theatre Club will provide all committee members and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification

- Users are obligated to report instances of non-compliance to the Burgess Hill Theatre Club Data Protection Officer.
- No access to any Burgess Hill Theatre Club IT resources and services will be provided without prior authentication.
- Password issuing, strength requirements, changing and control will be managed through formal processes.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by Burgess Hill Theatre Club policies, standards and guidelines.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, user account privileges and other methods as necessary.
- A formal process shall be conducted at regular intervals by data owners to review users' access rights. The review shall be logged.

28. Wireless Policy

Burgess Hill Theatre Club does not have a wireless network. If the need arises to use wireless technology it should be approved by Burgess Hill Theatre Club committee and the following wireless standards have to be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves Burgess Hill Theatre Club.
2. The firmware on the wireless devices has to be updated accordingly as per vendors release schedule
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.
6. An Inventory of authorized access points along with a business justification must be maintained. (Update Appendix B)

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

Hannah Wilson

_____

Officer Name (printed)

Data Protection Officer and Treasurer (Officer of the Club)

_____

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to Burgess Hill Theatre Club by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my service with Burgess Hill Theatre Club, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Committee that is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued service on Committee, I agree to abide by the policies and other requirements found in Burgess Hill Theatre Club security policy. I understand that non-compliance will be cause for disciplinary action up to and including termination of membership, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____

Employee Signature

Laurence Leng

_____

Officer Name (printed)

Secretary (Officer of the Club)

_____

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to Burgess Hill Theatre Club by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my service with Burgess Hill Theatre Club, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Committee that is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued service on Committee, I agree to abide by the policies and other requirements found in Burgess Hill Theatre Club security policy. I understand that non-compliance will be cause for disciplinary action up to and including termination of membership, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____

Employee Signature

Pippa Jones

_____

Officer Name (printed)

Chair (Officer of the Club)

_____

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to Burgess Hill Theatre Club by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my service with Burgess Hill Theatre Club, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Committee that is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued service on Committee, I agree to abide by the policies and other requirements found in Burgess Hill Theatre Club security policy. I understand that non-compliance will be cause for disciplinary action up to and including termination of membership, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____

Employee Signature

Appendix B

Asset/Device Name	Description	Owner/Approved User	Location
Barclaycard POS Device	M5000-016-BB TID: 26608397 Merchant number: 1593634	Hannah Wilson Laurence Leng Pippa Jones	Burgess Hill Theatre and other places of ticket or refreshment sales

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
Barclaycard		POS Device	Yes	06/02/2022