# Information Security Policy

## The Scottish Beekeepers' Association (SCIO)

Registered Charity No. SC009345

May 2019

# Contents

## 1. Introduction

This Policy Document encompasses all aspects of security surrounding personal and confidential information used and retained within the Scottish Beekeepers' Association (the organisation) and must be distributed to all Trustees, Authorised Officers, Sub-Committee Members, Volunteers, Consultants and Contractors to the organisation, including any Volunteers who may receive or handle information. All those issued this document must read it in its entirety and sign the form confirming they have read and understand this policy fully and the implications in relation to their access and use of information provided to the organisation. This document will be reviewed and updated by the Trustees on an annual basis or when relevant and distribute it as applicable.

## 2. Information Security Policy

The Scottish Beekeepers' Association handles personal and potentially confidential or sensitive information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Personal data is described along with other key definitions by the Information Commissioner Office and we request that you familiarise and keep yourself informed on these via the ICO website

https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees

The Scottish Beekeepers' Association commits to respecting the privacy of all its members, volunteers and customers and to protecting any data about them from outside parties. To this end Trustees are proactively working to providing and maintaining secure environments in which to process information so that we can meet these commitments.

Trustees, volunteers or anyone acting on behalf of the organisation may be required to handle confidential information. Confidential information includes but is not limited to personal information, and organisation data. Trustees, volunteers and anyone acting on behalf of the organisation should ensure they:

- Handle personal and confidential information in a manner that fits with their sensitivity;
- Do not disclose personal and confidential information unless authorised;
- Protect personal and confidential information;
- Keep passwords and accounts used for the purposes of the organisation in a secure manner;
- Request approval from The Trustees, one of which must be the IT Trustee prior to establishing any new software or hardware, third party connections, etc. ensuring appropriate security and information management policies are contracted;
- Do not install unauthorised software or hardware that will hold or process personal or confidential information provided to the organisation by its members, volunteers or cardholders, unless you have explicit Trustee approval;
- Always leave desks clear of personal and confidential information related to the organisation and its members and lock computer screens used for processing when unattended;
- Information security incidents must be reported, without delay, to the Trustee responsible for incident response locally – if in doubt this should be reported to General Secretary and President.
- Do not use e-mail, internet and other organisations' resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- We each have a responsibility for ensuring our organisation's systems and data are protected from

unauthorised access and improper use. If you are unclear about any of the detail herein you should seek advice and guidance from the Trustee aligned to area of activity related.

## 3. Acceptable Use Policy

The Trustees' intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to the Scottish Beekeepers' Association established culture of openness, trust and integrity. Trustees are committed to protecting the Trustees, Volunteers, Contractors, and the organisation from illegal or damaging actions by individuals, either knowingly or unknowingly. The Scottish Beekeepers' Association will maintain an approved list of technologies and individuals (Trustees, Authorised Officers, Sub-Committee Members, Volunteers, Contractors) with access to such devices as detailed in Appendix B.

- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors are responsible for exercising good judgment regarding the reasonableness of accessing and using personal or confidential information.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should ensure that they have appropriate knowledge and are authenticated for the use of technologies.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should take all necessary steps to prevent unauthorised access to personal and confidential information.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should ensure any related passwords are kept securely and do not share accounts, unless in exceptional and documented circumstances.
- Authorised users are responsible for the security of their passwords and accounts.
- All electronic devices, inclusive of PC's Laptops, mobile phones and portable storage devices used for the access and or processing of the organisations personal or confidential information should be secured with a password-protected screensaver with an automatic activation feature.
- All POS and PIN entry devices should be appropriately secured so they cannot be tampered with or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised whilst in transit.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors must use extreme caution when opening organisation related e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Anything of suspicion should be investigated locally and deleted and not forwarded on to other organisations authorised users.

## 4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by Trustees and authorised Officers and Volunteers will result in action, from warnings, to removal of position and possible membership (in line with the Scottish Beekeepers' Association Constitution). Claims of ignorance, good intentions or using poor judgment will not be acceptable as excuses for non-compliance.

## 5. Protect Stored Data

All data stored and handled by Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors must always be securely protected against unauthorised use. Any personal or confidential data that is no longer required by the organisation for business reasons must be discarded in a secure and

irrecoverable manner.

**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 for payment cards under any circumstance.

## 6. Information Classification

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

- **Confidential data** might include elements of personal data and or information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the organisation if disclosed or modified. **Confidential data includes payment or cardholder data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorised disclosure, sensitive to the running or objectives of the organisation;
- **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 functions that require access to cardholder data should be clearly defined.

- Any display of the card holder data should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as Permanent and or Primary Account Number(s) (PAN's), personal information and business data is restricted to Trustees and authorised Officers and Volunteers that have a legitimate need to view such information, these individuals should complete the form listed in Appendix A
- 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.
- The organisation 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.
    - The organisation will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
    - The organisation will monitor the Payment Card Industry Data Security Standard (PCI DSS) compliance status of any listed Service providers, via the annual production of their Compliance Certificate, which will be issued to the Treasurer.

## 8. Physical Security

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

- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors are responsible for exercising good judgment regarding the reasonableness of confidential data. If in any doubt, do not proceed.

- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should take all necessary steps to prevent unauthorised access to Confidential and internal use data which includes card holder data.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors should ensure that technologies should be used and setup in acceptable locations, that are secure and not in an open public space with a potential for theft or inappropriate observation of data being accessed.
- A list of devices that accept payment card data should be maintained (Appendix B).
- The list should include make, model and location of the device, the serial number or a unique identifier of the device and be updated when devices are added, removed or relocated
- Point of Sale (POS) devices surfaces should be periodically inspected to detect tampering or substitution.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors using the devices should be trained and aware of possible security issues whilst handling the POS devices
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors using the devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks, install new devices or replace devices.
- Trustees, Authorised Officers, Sub-Committee Members, Volunteers and Contractors using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the Shows and Publicity Officer.
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals. (Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.)
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered with or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and must be approved by the Trustees.
- All computers that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

## 9. Protect Data in Transit

All Personal, Confidential or internal use data must be protected securely if it is to be transported physically or electronically.

- Confidential or internal use data should never be sent over the internet via instant chat or social media unless you have direct consent to do so from all individuals involved. Personal or Confidential Data that is transmitted via email should be limited and where possible via files that have encryption applied, where possible.
- If there is a business justification to send Confidential or internal use 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 Personal, Confidential or Internal Use data to another location must be authorised by the relevant Trustee, and logged before transportation. Only secure courier services may be used for the transportation of such media. The status of the shipment should be recordable and monitored until it has been delivered to its new location and signed for.

## 10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the organisation, regardless of the media or application type on which it is stored.
- A process must exist to permanently delete any electronically held data, when no longer required.
- All hard copies of Personal, Confidential or Internal Use data must be manually destroyed as and when no longer required for valid and justified business reasons (i.e. once transactions have been confirmed as successful). A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The organisation will identify the process for the destruction of hardcopy (paper) materials as part of Appendix C. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The organisation will have documented procedures for the destruction of electronic media and requires:
    - All Personal, Confidential or internal use 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 Personal and Confidential information awaiting destruction must be held in lockable storage clearly marked “To Be Shredded/Incinerated” - access to these containers must be restricted.

## 11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into organisational practice to maintain a high level of security awareness. The protection of Personal, Confidential or Internal use data requires regular instruction and or training of all Trustees, authorised Officers, identified Volunteers and contractors.

- Review handling procedures for sensitive information including use of POS devices and hold periodic security awareness meetings to incorporate these procedures into practice.
- Distribute this security policy document to all Trustees, authorised Officers, identified Volunteers and contractors to read. It is required that all Trustees, authorised Officers, identified Volunteers and contractors confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS) and present their compliance certificates annually.
- All third parties with access to Personal and or Confidential data are contractually obligated to comply with GDPR and annually provide evidence that they do so.
- This and any associated policies or procedures must be reviewed annually and updated as needed.
- Instruct, through this policy, that all Trustees and any identified Officers use a standard email Signatory (electronic) format which will include the following SBA Disclaimer statement: -
    - The information contained within this e-mail and in any attachment is confidential and privileged. If you are not the intended recipient, please destroy this message, delete any copies held including any attachments and notify the sender immediately of the error. You should not retain, copy or use this e-mail for any purposes nor disclose any part of it to any other person other than the originator.

## 12. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to communications or information including manual or electronic processing systems. If deliberate, the attacker could be a malicious stranger, or disgruntled Trustees, authorised Officers, identified Volunteers and contractors, and their intention might be to steal information or money, or just to damage our organisation. This also relates to accidental actions of any Trustees, authorised Officers, identified Volunteers and contractors, which involves sensitive data release inappropriately as guided by this policy.

**Incident Response Notification**

1. In the event of a suspected security breach, alert the relevant Trustee related to the area or function you are participating in.
2. The Trustee will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Trustee will alert fellow Trustees and begin informing all relevant parties that may be affected by the compromise, including any commitment made in the organisation's Privacy Statement.
4. If the incident relates to cardholder details the following steps must be taken:

**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 via 0800-89-1725

- 0800-89-1725.
- For more Information visit: https://www.visa.co.uk/contact-us.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
      - Identify systems analysed if applicable. Include Domain Name System (DNS)

names, Internet Protocol (IP) addresses, Operating System (OS) version, Function of system(s)

c. Timeframe of compromise
d. Any data exported by intruder
e. Establish how and source of compromise
f. 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.)
g. 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

**MasterCard Steps:**

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at
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.

**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

## 13. Third party access to card holder data

- All third-party companies providing critical services which includes data hosting to the organisation must provide a contract which contains suitable evidence of relevant Data Security, such as in the form of an Information Asset Register and Privacy Statement or Security 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. 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.

## 14. User Access Management

- Access to Personal, Confidential or Internal Use data, including any data mentioned in the Scottish Beekeepers' Association Privacy Statement is controlled through the collation of Appendix C which is agreed by the Trustees and reviewed regularly.
- Each 'user' who may be Trustees, authorised Officers, identified Volunteers and contractors is identified along with the data they will be accessing for any purpose in the organisation's Information Asset Register (IAR) and will clearly identify who is accessing what sensitive data for what purpose, and the 'user' is made responsible for their actions. This is available in Appendix C.
- Access to all the organisation's information and data, including any in systems, can only be started after proper procedures are completed, the access recorded in the IAR, and this policy read and a copy of Appendix A signed.
- As soon as an individual is no longer acting on behalf of the organisation, all his/her system logons must be immediately revoked, and any media returned or witnessed to be destroyed following the above clause.

## Appendix A – Agreement to Comply Form – Agreement to Comply with Information Security Policy

_____

**Name (printed)**

I agree to take all reasonable precautions to assure that the organisation's internal information, or information that has been entrusted to the organisation by third parties such as members and customers, will not be disclosed to unauthorised persons. At the end of my tenure as trustee, or I no longer am a member of the organisation, 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 relevant Trustee.

I have access to a copy of the Information Security Policy, I have read and understand this policy, and I understand how it impacts my role within the organisation. As a condition of continued tenure as a trustee or officer, I agree to abide by the policy and other requirements found in the organisation's information security policy. I understand that non-compliance will be cause for disciplinary action as per the organisation's Constitution, and perhaps criminal and/or civil penalties. I also agree to promptly report all violations or suspected violations of information security policies to the General Secretary.

_____

**Signature**

## Appendix B – Electronic Devices – Used to Hold Personal or Sensitive Data

| Asset/Device Name | Description | Owner/Approved User | Location |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## List of Service Providers (Contracted Services where relevant)

| Name of Service Provider | Contact Details | Services Provided | PCI DSS Compliant (if relevant) Including Date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Appendix C

**GDPR Information Asset Register for**

# The Scottish Beekeepers' Association (SCIO) Registered Charity No. SC

**Date completed/reviewed: June 2019 (reviewed xxx)**
**Completed by: XXXX Trustee**

Under the new principle of data accountability, organisations need to be able to demonstrate their compliance with the
maintain records of what personal data we hold, who has access to it and how it is securely stored. Completing this
recommended to demonstrate good security procedures and designed to complement the SBA Information Security Po

| Type of Personal, Confidential Information | Location of data | Who has access to the data and for what purpose* | Data retention |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**The President, Vice President, General Secretary and Treasurer may not have regularly access to data listed for day to day organisational activities under their 'office'. However, s*
*investigation for whatever reason, any of The President, Vice President, General Secretary and Treasurer will request access to any information held by the organisation for this spe*