Information Security Policy

for

Beeswift Ltd.

Policy effective from 11/06/2018

Last Updated by Ebit Consultancy Ltd. on behalf of Beeswift Ltd.

Version History

Change Date	Author	Change	Next Review Date
11/06/2018	EbitConsultancy Ltd.	Initial Version	11/06/2019
10/06/2019	Beeswift Ltd	Annual Review	11/06/2020
11/06/2020	Beeswift Ltd	Annual Review	11/06/2021
11/06/2021	Beeswift Ltd	Annual Review	11/06/2022

Contents

1 PURPOSE 5

1.1 Introduction 5
1.2 Why this policy exists 5
1.3 Intended Audience 5
1.4 Data Protection Law 5

2 PEOPLE, RISKS AND RESPONSIBILITIES 6

2.1 Policy Scope 6
2.2 Data Protection Risks 7
2.3 Responsibilities 7

3 WHAT IS BEING PROTECTED 8

4 SECURITY PRINCIPLES 8

4.1 Confidentiality 8
4.2 Integrity 9
4.3 Availability 9
4.4 Regular Assessment 9
4.5 Data Protection Impact Assessment 9
4.6 Overall Objectives 9

5 CONFIGURATION 10

5.1 Network Protection 10
5.1.1 Firewall Configuration 10
5.1.2 Router Configuration 10
5.1.3 Content Monitoring 10
5.1.4 Email Monitoring 10
5.2 Device Protection 10
5.2.1 General rules 10
5.2.2 Servers 11
5.2.3 Computers and Laptops 11
5.2.4 Smartphones and Tablets 12
5.2.5 "Bring-your-own" Devices 12
5.3 User Protection 12
5.4 Role-based Security 13
5.5 Data Protection 13
5.6 Data Destruction 13

6 APPROVED CLOUD SERVICE SELECTION 13

6.1 Criteria 13
6.2 Providers 13

7 DATA PROCESSORS 14

7.1 Company Responsibility 14
7.2 Criteria 14
7.3 Suppliers who do not meet the criteria 15

8 MONITORING 15

8.1 NETWORK MONITORING 15
8.2 WEBSITE MONITORING 15
8.3 DATABASE ACTIVITY MONITORING 15
8.4 INTERNET ACTIVITY 15
8.5 EMAIL ACTIVITY 15
8.6 DATA LOSS PREVENTION 16
9 INCIDENT HANDLING 16
10 RISK ASSESSMENTS 17
10.1 WHEN TO DO ONE 17
10.2 WHEN SHOULD THEY BE REVIEWED 17
10.3 WHAT SHOULD IT INCLUDE 17

1 Purpose

1.1 Introduction

Beeswift Ltd. needs to ensure all its systems, data and intellectual property, and data and intellectual property entrusted to it by its customers and suppliers are safe, secure and available.

This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this information must be collected, handled and stored to meet the company's data protection standards, and to comply with the law.

1.2 Why this policy exists

This security protection policy ensures Beeswift Ltd.:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

1.3 Intended Audience

This document is intended to be used by the Data Protection Officer and technical staff.

1.4 Data Protection Law

The European Union General Data Protection Regulation (GDPR) 2018 (to be enforced in the UK as part of the Data Protection Bill 2017) describes how organisations – including Beeswift Ltd. – must collect, handle and store personal information.

GDPR supersedes all national regulations including the U.K. Data Protection Act 1998 providing a revised set of rules and principles. As this is more strictly defined and enforced than existing national rules, this policy is in compliance with GDPR.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation is underpinned by six important principles. These say personal data must:

1) processed lawfully, fairly and in a transparent manner in relation to individuals;

2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As a Data Controller, Beeswift Ltd. is responsible for and be able to demonstrate compliance with the principles.

2 People, Risks and Responsibilities

2.1 Policy Scope

This policy applies to:

- The head office of Beeswift Ltd.
- All staff and volunteers of Beeswift Ltd. wherever they are working
- All contractors, suppliers and other people working on behalf of Beeswift Ltd.

It applies to all systems, devices and cloud services used by Beeswift Ltd. as part of its normal operations.

2.2 Data Protection Risks

This policy helps to protect Beeswift Ltd. from some very real security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

2.3 Responsibilities

Everyone who works for, or with Beeswift Ltd. has some responsibility for ensuring data is collected, stored and handled appropriately. Beeswift Ltd. has responsibility to ensure appropriate measures are in place to protect the data and its systems from external interference.

Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Within the business, the following roles have key areas of responsibility:

- the board of directors is ultimately responsible for ensuring that Beeswift Ltd. meets its legal obligations.
- David Griffin, acting as The Data Protection Officer for Beeswift Ltd. is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - arranging data protection training and advice for the people covered by this policy.
    - Dealing with requests from individuals to see the data Beeswift Ltd. holds about them (also called ‘subject access requests’).
    - checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
- faIT UK Ltd. (The IT Provider), is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

3 What is being protected

The purpose of the policy is to ensure all systems used by Beeswift Ltd. are configured to protect:

- The data and intellectual property entrusted to it by its customers
- All personal data
- The data and intellectual property of Beeswift Ltd.
- All communication with suppliers and customers to ensure malware is not propagated
- The reputation of Beeswift Ltd.

This is not an exhaustive list but the intention is to ensure only authorised individuals within Beeswift Ltd.

- have appropriate access to data,
- can do so safely
- have the correct tools to do so

4 Security Principles

Beeswift Ltd. has a responsibility to make sure their systems are robust, secure and available as and when required, and that they can be recovered quickly to minimise disruption to its customers and employees.

Information Security has three basic principles detailed as follows:

4.1 Confidentiality

Confidentiality is about ensuring information is only available to those who should be able to see it.

Beeswift Ltd. enforces this through job related security roles which determine what information is available at what point.

4.2 Integrity

Integrity is about ensuring the information being used is correct, up-to-date and reliable. The information must not be able to be altered or deleted inadvertently or maliciously.

Beeswift Ltd. ensures this by the processes defined in the Data Protection Policy, supported by security roles and a reliable and robust backup and recovery mechanism (because we are all human).

4.3 Availability

Information should be available to those who need it, how, where and when they need it.

Beeswift Ltd. uses VEAM Backups to an offsite location, There are also backups which occur for Varnet to a Magnetic disk, to the SAN and to an offsite location.

Changes to this approach are planned and will be implemented as soon as practicable.

4.4 Regular Assessment

It is imperative that the security measures are tested regularly (between every 3 and 6 months) to ensure the technical, procedural and education aspects of information security remain effective.

This includes staff as well as technical measures.

4.5 Data Protection Impact Assessment

Where a significant change in the manner in which information is held (such as a change in technology, or change of storage location), a new technology is introduced which holds personal information or the company experiences a breach, a Data Protection Impact Assessment must be carried out.

This will detail the technologies, locations, access privileges, transfers and risks involved in the change and provide an assessment on the scale of the risks involved and the actions required to mitigate them.

4.6 Overall Objectives

This can be summarised as “stopping the bad guys from getting in and stopping our data from leaking out”.

It is also about ensuring the employees have systems which allow them to work efficiently, effectively and safely.

5 Configuration

5.1 Network Protection

Secure network access is a key element of modern day working. With so many devices connected to and depending on each other, ensuring they are able to communicate with each other without interference or interception is critical to business success.

To achieve this, it is vital that all network technology under control of Beeswift Ltd. is configured to be as safe and secure as possible whilst not prohibiting valid usage of internet resources.

Configuration and management of the Network security systems is outsourced to an approved supplier, therefore the Beeswift Ltd. must ensure the supplier is responsible and responsive.

5.1.1 Firewall Configuration

The firewalls should be and are configured to prohibit all incoming access except via secure protocols and methods. If possible, they should be set to the most restrictive settings but this will need to be balanced against tools such as VOIP devices and the VPN.

No network services are to be broadcast out onto the wider internet.

5.1.2 Router Configuration

All default passwords have been changed, and usernames where this is possible. Review all default settings and if combined with a firewall, ensure the settings are as robust and prohibitive as possible.

5.1.3 Content Monitoring

A combination of firewall products is used to protect devices from known-black listed, spam, malware and undesirable sites.

5.1.4 Email Monitoring

A number of products are to be used for email content filtering to provide a level of email monitoring including spam and malware detection.

5.2 Device Protection

5.2.1 General rules

The following rules apply to all devices and systems used by Beeswift Ltd..

- All software to be installed on Beeswift Ltd. devices must be purchased and downloaded directly from a reputable supplier using their managed “App stores” or officially approved download sites.

- No software is to be acquired or installed from any other source. End-users do not have sufficient access privileges to carry out such activity.
- All software is to be logged in the Software Asset Register detailing:
    - Where it has been obtained from
    - Any licensing information
    - Why it was acquired/What purpose does it serve?
    - Where is it installed?
- The operating system and all applications are to be configured to automatically update. Where applications must be updated manually through the app store, this must be done weekly.
- All devices are to have Anti-Malware software installed (where this exists)
- All devices are to have firewalls enabled and configured to the most restrictive settings only allowing permitted services to open outgoing connections.
- All operating system and data disks are to be encrypted during installation and certainly prior to any data or intellectual property being copied onto them.

5.2.2 Servers

Servers are to be configured according to the general rules and additionally:

- Servers should be configured with a minimal operating system installation and only sufficient additional packages or software to operate for the purpose they exist for.
- User accounts must be kept to a minimum with minimum password length of 16 characters.
- No service usernames or passwords are to be kept in any configuration files for any purpose unless they are encrypted.
- Servers are not to be configured to hold any personal information whether directly or indirectly.

5.2.3 Computers and Laptops

Computers and laptop devices are to be configured according to the general rules and additionally:

- Connection of any form of USB storage device is prohibited.

5.2.4 Smartphones and Tablets

Smartphones and tablet devices are to be configured according to the general rules and additionally:-

- Company devices may be configured to access electronic mail and use the company VPN.
- No company information assets are to be copied onto these devices under any circumstances.
- Backups of these devices should be via appropriate software on the internet (such as Apple iCloud, or equivalent)
- All such devices owned by Beeswift Ltd. must be configured with a remote erase or kill switch to enable the devices to be rendered useless if stolen or lost.
- All devices must use a minimum 6-digit passcode and be configured to automatically lock after 1 minute.

5.2.5 "Bring-your-own" Devices

Employees may bring their own devices which may make use of any public Beeswift Ltd. network facilities. The devices are not to be used to access company data or intellectual property but may connect to the email system using the webmail portal.

The email portal must be configured to prevent 3rd-party apps from connecting to or accessing company email.

5.3 User Protection

All users of Beeswift Ltd. systems should expect to have the right tools for them to fulfil their jobs and that they should be able to do so safely and securely without onerous data protection or security processes and procedures.

Equally they should be expected to fulfil their part of the agreement to which they are expected:

- to use passwords which are 9 characters or more in length and be prepared to change them on a regular basis. Password security must be configured to allow as wide a combination of letters, numbers, special characters and spaces as possible on that device and operating system. However, forcing minimum combinations of letters will not be enforced.
- to follow the rules for using Beeswift Ltd. equipment and systems and not connect anything they shouldn't in a way that isn't explicitly allowed

5.4 Role-based Security

To enforce confidentiality of information and ensure staff only have access to the information they need, a top-down security model should be enforced across all systems where this is practicable. This can ensure staff only have access to systems and information which they require for their jobs and nothing else, also simplifying staff transferring between jobs.

This will also simplify auditing and risk assessments.

At present this is only enforced within the accounts team (who are also responsible for Human Resources) owing to technical limitations on the main business network.

5.5 Data Protection

Beeswift Ltd. takes this very important so it is covered in greater detail in the Data Protection Policy.

5.6 Data Destruction

All data held electronically should be deleted rather than just placed in a Waste Basket/Trash Can/Recycle Bin. Faulty or old hard drives/media are sent away for destruction by an approved data recycler who provide data destruction notices.

Network Administrators should periodically clear all user 'Trash Cans/Recycle Bins'.

All information held as a physical copy should be destroyed through either office based shredding devices or through outsourced secure destruction specialists.

6 Approved Cloud Service Selection

6.1 Criteria

All cloud suppliers must accept their responsibility as service providers for the data they have in their care. They must clearly state that they accept their responsibility as a data processor under the EU GDPR and that they have taken appropriate security measures to protect Beeswift Ltd.'s data whilst at rest on their storage and in transit.

6.2 Providers

Beeswift Ltd. only use the following cloud service providers:

Provider	Usage	Storage Location	Encrypted	GDPR Compliant	Data Processor Statement
DropBox	Shared File Storage (for External Use Only)	Europe	Yes	Yes	Yes
Sage	Accounting system	Europe	Yes	Yes	Yes

7 Data Processors

7.1 Company Responsibility

Beeswift Ltd. has a responsibility to ensure any personal information it controls is managed both inside the perimeter of the business network and by any companies it uses to process that information on its behalf, to the same standards and expectations that it sets, and within the requirements of the GDPR. In this case, GDPR is used to manage processing which may be performed within the European Union rather than just within the borders of the United Kingdom.

7.2 Criteria

All data processors must be assessed against the following criteria and match or exceed them in every area:

- Mandatory encrypted transfers of information between Beeswift Ltd. and the company;
- Store and process all entrusted personal data in a secure manner and with due respect for the privacy of the individuals;
- Must have clear processes and procedures for managing Subject Access Requests;
- Must have a published GDPR compliance statement;
- Must include clauses within their contracts for the Data Controller/Data Processor relationship;
- Must be prepared to open themselves up to being audited if the need arises;
- There must be an individual within the company who is accountable for Data Protection and Privacy.

7.3 Suppliers who do not meet the criteria

Any business which takes Data Protection seriously will have no problems adhering to these criteria. However, it is acknowledged that there will be a period of transition toward Data Privacy practices and that not all service providers will be compliant to start off with.

There must be a deliberate judgment made as to the risk to Beeswift Ltd. if they were to suffer a data breach at the hands of a non-compliant organisation. The final decision for this lies with the Data Protection Officer but should their advice be ignored, the company directors will then be judged liable for the breach.

If the processing organisation is not immediately compliant, Beeswift Ltd. can give that organisation some breathing space but they must monitor the supplier and be prepared to walk away if they have not achieved compliance after a sensible amount of time.

8 Monitoring

8.1 Network Monitoring

Ubiquiti networking software monitors and logs all devices connected to our network with times and device names for reporting on internal devices connecting to our network .

8.2 Website Monitoring

On the main website, page requests and errors are recorded and these are downloaded from the webserver on a weekly basis for analysis.

8.3 Database Activity Monitoring

Beeswift Ltd. does not currently use any in-house database systems.

8.4 Internet Activity

The combination of firewall and device website proxy software provides website filtering to prevent the majority of undesirable sites from being accessible within the business. This combination uses a mixture of rules and blacklists to determine what is and isn't allowed through.

The rules and blacklist should be reviewed regularly and ideally automatically updated from industry standard lists.

8.5 Email Activity

Beeswift Ltd. uses an onsite Microsoft Exchange server for the provision of email services. This system is hosted on their own site and is not cloud based.

Communication is further monitored through the company's main firewall.

At present, there is no filtering of outgoing email to prevent data leakage.

8.6 Data Loss Prevention

All Laptops that are allowed off site are fully encrypted (Bitlocker) so any data is useless in the event of Laptop theft or being lost. We also have the option of being able to issue a (wipe command) to erase the device in this eventuality.

Beeswift have heavily invested in its internal and gateway level security to guard against virus, malware, phishing, brute force attacks, exploit defence, fileless attacks, email security and given staff training in secure procedures.

Beeswift's internet gateway is routinely penetration attacked by a 3rd party as required by our Bank who requires us to be PCI compliant. We have strict rules to follow to meet their certification

Information is key to Beeswift. To that end we have heavily invested in a robust data backup system which frequently copies our data to both on-site and off-site locations so that in the event of a hardware/software/theft/act of god incident that resulted in live data loss a data retrieval job could be fired off and data restoration could be completed in a timely manner.

Data is transmitted offsite via secure VPN tunnels to equipment owned by Beeswift at one of our IT suppliers premises. Our data doesn't leave our own equipment. We regularly test our backups to make sure we can restore data to ensure successful data retrievals.

9 Incident Handling

This is detailed separately in the Breach Handling Manual.

10 Risk Assessments

10.1 When to do one

Beeswift Ltd. must conduct information security risk assessments as follows:

- prior to making any significant change to Beeswift Ltd.'s systems, their configurations or any change of the underlying infrastructure;
- prior to undertaking any work which may require storage or processing of personal data in relation to, or on behalf of new customers to ensure all communication and processes between Beeswift Ltd. and the customer are safe and secure.

10.2 When should they be reviewed

All risk assessments should be reviewed and potentially revised according to the following schedule:

- immediately following a breach;
- immediately following a mass internet attack (such as the WannaCry outbreak in May 2017) to ensure all defences are robust;
- at least every 6 months.

These reviews are to be logged in the risk register.

10.3 What should it include

The risk assessment must be an overarching information security risk document covering all potential risks in the current Beeswift Ltd. infrastructure and systems.

This must include:

- all boundaries between Beeswift Ltd. and the wider internet;
- all data storage areas (including areas containing intellectual property and company confidential information);

- all data flows between different devices;
- all data flows between storage or devices and individuals;
- all data access from outside Beeswift Ltd.;

For E.U. G.D.P.R compliance, the risk assessment must also include a Data Privacy Impact Assessment to ensure any changes to technology or processes are evaluated for Data Privacy issues.