Information Security Policy

Policy title:	**Minted Box INFORMATION SECURITY POLICY**

Issue date:	23/11/2018	**Date policy is to be reviewed:**	23/11/2019

Version: 1.1	**Issued by:** Peter Elliot & James Alvarez

Scope:	Covering the entities of Minted Box Ltd

Associated documentation:	Register for Physical Assets Register for Administration Accounts Incident Register
Appendices:	None
Approved by:	Iain Bell and James Alvarez
Date:	

Review and consultation process:	Annually from issue date above
Responsibility for Implementation & Training:	Responsibility for implementation lies with named business owners above

Revisions:			
Date	**Revision**	**Author:**	**Description:**
		Peter Elliot	First revision

Distribution	In PDF form by attachment to email to employees, suppliers, clients and auditors.

Contents

1. Introduction 1
2. Aim and Scope of this policy 1
3. Responsibilities 1
4. Legislation 2
5. Personnel Security 2
Contracts of Employment 2
Information Security Awareness and Training 3
Intellectual Property Rights 3
6. Access Management 3
Physical Access 3
Identity and passwords 3
User Access 4
Administrator-level access 4
Application Access 4
Hardware Access 4
System Perimeter access (firewalls) 4
Monitoring System Access and Use 5
7. Asset Management 5
Asset Records and Management 5
Removable media 5
Mobile working 6
Personal devices / Bring Your Own Device (BYOD) 6
Social Media 6
8. Physical and Environmental Management 7
9. Operations Management 7
System Change Control 7
Accreditation 7
Software Management 7
Local Data Storage 7
External Cloud Services 8
Protection from Malicious Software 8
Application Whitelisting 8
Application sandboxing 8
Vulnerability scanning 9
10. Response 9
Information security incidents 9
Reporting 9
Further Information 9

1. Introduction

This information security policy is a key component of Minted Box management framework. It sets out the requirements and responsibilities for maintaining the security of information within Minted Box. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day. This policy will also apply to any third-party organisations who are required to access Minted Box systems for management and maintenance purposes.

2. Aim and Scope of this policy

- The aims of this policy are to set out the rules governing the secure management of our information assets by:
    - preserving the **confidentiality, integrity and availability** of our business information
    - ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies
    - ensuring an approach to security in which all members of staff fully understand their own **responsibilities**
    - creating and maintaining within the organisation a level of **awareness** of the need for information and cyber security
    - detailing how to **protect** the information assets under our control
- This policy applies to all information/data, information systems, networks, applications, locations and staff of Minted Box or supplied under contract to it.

3. Responsibilities

- Ultimate responsibility for information security rests with the Board of Minted Box, on a day-to-day basis the Compliance Officer shall be responsible for managing and implementing the policy and related procedures.
- Responsibility for maintaining this Policy is held by the Compliance Officer. The Policy shall be reviewed by the Compliance Officer at least annually.
- The Compliance Officer is responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:-
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters

- All staff shall comply with the information security policy and must understand their responsibilities to protect the company's data. Failure to do so may result in disciplinary action.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contract shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4. Legislation

- Minted Box is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.
- The requirement to comply with legislation shall be devolved to employees and agents of Minted Box, who may be held personally accountable for any breaches of information security for which they are responsible.
- In particular, Minted Box is required to comply with:
  - The Data Protection Act (1998)
  - The Data Protection (Processing of Sensitive Personal Data) Order 2000.
  - The General Data Protection Regulation (EU, May 2018)
  - The Copyright, Designs and Patents Act (1988)
  - The Computer Misuse Act (1990)
  - Regulation of Investigatory Powers Act 2000
  - Freedom of Information Act 2000

5. Personnel Security

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.
- Information security expectations of staff shall be included within appropriate job definitions.
- Whenever a staff member leaves the company their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Information security awareness training shall be included in the staff induction process
- An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the Compliance Officer. Individual and Minted Box intellectual property rights shall be protected at all times.
- Users breaching this requirement may be subject to disciplinary action.

6. Access Management

Physical Access

- Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

- Passwords must offer an adequate level of security to protect systems and data
- Passwords must be promptly changed if the user knows or suspects they have been compromised.
- Where available, password lockouts or timeouts shall be implemented:
    - lock accounts after no more than 10 unsuccessful attempts
    - limit the number of guesses allowed in a specified time period to no more than 10 guesses within 5 minutes
- All passwords shall consist of four words of four or more letters not separated by spaces. Each word must contain at least one capital letter.
    - All administrator-level passwords shall use two-factor authentication where available to provide additional security
    - All users shall use uniquely named user accounts
    - Generic user accounts that are used by more than one person or service shall not be used.
    - All Users are advised:

- how to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet).
- not to choose common passwords (list maybe provided)
- not to use the same password anywhere else, at work or at home.
- where and how they may record passwords to store and retrieve them securely — e.g. in a sealed envelope in a secure cupboard or by using a recommended password manager
- which passwords they really must memorise and not record anywhere, such as a password manager password

User Access

- Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the Compliance Officer
- A list of individuals with administrator-level access shall be held by the Compliance Officer and shall be reviewed each time there is a change.
- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Access to the network shall be restricted to authorised devices only. Authorisation will be provided by the Compliance Officer following a risk assessment.

System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.

- All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy.
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised by the Compliance Officer. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- The business reserves the right to monitor any systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

7. Asset Management

Asset Records and Management

- An accurate record of physical information assets, including source, ownership, modification and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.

Removable media

- Removable media (such as USB memory sticks and recordable CDs/DVDs) shall not be used to store business data or connected to any business systems without the express permission of the Compliance Officer.
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the Compliance Officer before they may be used on business systems. Such media must be scanned by anti-virus before being used
- Users breaching these requirements may be subject to disciplinary action

Mobile working

- Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements
- Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Compliance Officer.
- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.
- Users must inform the Compliance Officer immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

- Where necessary, staff may use personal mobile phones to access business email. This usage must be authorised by the Compliance Officer. The device must be configured to comply with the mobile working section and other relevant sections of this policy.
- Personal mobile phones may connect to guest wi-fi only when on business premises, unless authorised to access the company network for business purposes, such as testing, but only with the express permission of the Compliance Officer.
- No other personal devices are to be used to access business information

Social Media

- Social media may only be used for business purposes by using official business social media accounts with authorisation from the Board of Directors. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.
- Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.
- Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the Compliance Officer.
- Users breaching this requirement may be subject to disciplinary action.

8. Physical and Environmental Management

- In order to minimise loss of, or damage to, all assets, access to equipment shall be limited to authorised individuals only.
- Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

9. Operations Management

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the Compliance Officer.

Accreditation

- Minted Box shall ensure that all new and modified information systems, applications and networks include security provisions in line with this Policy.

Software Management

- All application software, operating systems and firmware shall be:
  - licensed and supported,
  - removed from devices when no longer supported,
  - patched within 7 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’
- Only software which has a valid business reason for its use shall be installed on devices used for business purposes
- Users shall not install software or other active code on the devices containing business information without permission from the Compliance Officer.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

Local Data Storage

- Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals.
- A backup copy shall be held in a different physical location to the business premises
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External Cloud Services

- Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

- The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All in-scope devices shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily
- The software must be configured to scan files automatically upon access
- The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
- The software must prevent connections to malicious websites on the Internet (by means of blacklisting, for example) — unless there is a clear, documented business need and the Applicant understands and accepts the associated risk.

Application Whitelisting

- Only approved applications, restricted by code signing, are allowed to execute on devices. The Compliance Officer shall:
    - actively approve such applications before deploying them to devices.
    - maintain a current list of approved applications.

Application sandboxing

- All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user. This includes:
    - other sandboxed applications,
    - data stores, such as those holding documents and photos,
    - sensitive peripherals, such as the camera, microphone and GPS,

- local network access.

Vulnerability scanning

- The business shall have at least a monthly vulnerability scan of all external IP addresses carried out by a suitable external company
- The business shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities
- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

10. Response

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the Compliance Officer
- If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Compliance Officer
- Information security incidents shall be recorded in the Security Incident Log and investigated by the Compliance Officer to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

Reporting

- The Compliance Officer shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

Further Information

- Further information and guidance on this policy can be obtained from the Compliance Officer, James Alvarez at compliance@mintedbox.com. Comments and suggestions to improve security are always welcome.

Policy approved by:

Board Director (1) – James Alvarez

Signature Date 23/11/2018

Board Director (2) – Iain Bell

Signature Date 23/11/2018

On behalf of Minted Box Ltd.