Screenworks Ltd
IT Security Policy

Version: 2.0

Author: David Fox, IT Manager

Table of Contents

1. Version Control

Issue Date:	08 August 2022	
Version:	2.0	
Issued by:	David Fox	IT Manager
Approved By:	*Internal Confidential*	*Internal Confidential*
Date:	08 August 2022	
Next Review Date:	08 February 2023	
Implementation and Training:	David Fox	IT Manager

2. Version History

Please Refer To The Section Located At The End Of This Document: Document Revision History

3. References

Ref #	Reference	Version
1	Government Cyber Essentials Website	16 January 2018
2		
3		

4. Introduction

The Screenworks IT Security Policy is a key component of the overall business management framework. The policy provides detailed guidance and information regarding the appropriate and secure use of IT resources within the business, along with their management and care.

Implementation of the Screenworks IT Security Policy is the responsibility of every employee and visitor coming into Screenworks who will be accessing any IT resource within the Screenworks network.

Failure to adhere to any part of the IT Security Policy places the business at risk and exposed to any number of significant threats including (but not limited to):

- Malicious code entering the network;
- Threats from Hackers and Phishing Attacks
- Unauthorised access to systems and data;
- Unauthorised persons gaining access to confidential information;
- Data leakage and compromise of confidentiality, integrity and availability of company CONFIDENTIAL data.

The adverse business impacts potentially flowing from these risks include:

- Loss of availability of key systems and/or loss of data.
- Interruption of normal business operations and resultant loss of revenue.
- Damage to Screenworks Ltd reputation and loss of confidence amongst customers, employees, business partners and parent company.
- Allegations of poor corporate governance resulting in adverse publicity and parent company dissatisfaction.
- Confidential business information falling into the hands of competitors and other third parties.
- Reputational damage to Screenworks Ltd.
- Compliance with these policies, procedures and standards is therefore required from all persons who have access to any of Screenworks Ltd IT infrastructure or information assets. This includes third parties (e.g., contractors, business partners and – in some cases – customers) as well as employees.

5. Objectives, Aim and Scope

Objectives

The objective of this Information Security Policy is to help preserve the confidentiality, integrity and availability of our business information, based upon a risk assessment and an understanding of our tolerance for risk.

Policy Aim

The aim of this policy is to set out the rules governing the secure management of our information assets.

It will achieve this by 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 security as an integral part of the day to day business and protecting information assets under the control of the organisation.

Scope

This policy applies to all information, information systems, networks, applications and users of Screenworks Ltd or supplied under contract to it.

6. Responsibilities

Ultimate responsibility for information security rests with the Co-Founders of Screenworks Ltd; Information Security Employees shall be responsible for managing and implementing the policy and related procedures.

Line Managers are responsible for ensuring that their permanent and 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 information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

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.

Contracts with external parties that allow access to the organisation's information systems shall be in place before access is allowed. These contracts shall aim to ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

Implementation of the Information Security Management Forum (ISMF)

Screenworks Ltd shall implement an ISMF that shall meet on a regular basis and at least annually.

ISMF Terms of Reference

To take overall responsibility for Information Security Management within the Information Management System Scope. This shall include representation from:

- IT Security
- Physical Security
- Human Resources
- Facilities Management
- The Business via Senior Management.

The ISMF will:

- Define ownership and responsibility for Information Security Policy and Procedures
- Set Information Security Policy within Screenworks Ltd
- Have representation on the management board meetings to address security issues.

7. Legislation

Screenworks Ltd is required to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Screenworks Ltd, who may be held personally accountable for any breaches of information security for which they may be held responsible. Screenworks Ltd shall comply with the following legislation and other legislation as appropriate:

- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- GDPR

9. Personnel Security

Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all prospective staff members shall be subject to a level of security screening appropriate to their role. This shall be conducted by the HR function with advice and input from the Screenworks Ltd Accounts Manager. As a minimum this should include:

- Verification of identity;
- Employment history (for a minimum of the past three years);
- Verification of nationality and immigration status.

Information security expectations of staff shall be included within appropriate job definitions and that any breach of information security controls may be considered a misdemeanour under Screenworks Ltd disciplinary policy, and which in turn might, under specific circumstances, result in dismissal.

All access rights shall be removed immediately on termination of contract.

Information Security Awareness Training

Information security awareness training shall be included in the staff induction process.
Users shall be made aware of the procedures applicable to them and refreshed regularly.
An on-going awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Intellectual Property Rights

The organisation shall ensure that all software is properly licensed and approved by the IT Manager. Individual and Screenworks Ltd IPR shall be protected at all times. Users breaching this requirement may be subject to disciplinary action.

Social Media

Social media may be used for business purposes on condition that no CONFIDENTIAL or potentially CONFIDENTIAL material, IP or similar material is disclosed. Users must 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 IT Manager. Users breaching this requirement may be subject to disciplinary action.

10. Asset Management

Removable media

The use of removable media is permitted within the Screenworks Ltd but shall be restricted to official use only and subject to anti-virus scanning prior to transferring any data.

Removable media from external sources

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the IT Manager before they may be used on business systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

Mobile devices (e.g. phones, tablets, laptops etc.)

Use of mobile devices for business purposes (privately or business owned) requires the approval of the IT Manager before they may be used. Such devices must at a minimum have anti-malware software installed and updated daily, have pin, password or other authentication installed, be encrypted wherever possible and be capable of being remotely tracked and wiped. Users must inform a member of the IT team immediately if the device is lost or stolen and the device must be subsequently completely wiped.

CONFIDENTIAL Information Assets

Screenworks Ltd shall identify particularly valuable or CONFIDENTIAL information assets, based upon the results of a risk assessment. The classification CONFIDENTIAL shall be marked on all such material (in document and electronic form) and shall be held securely at all times. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Data in electronic form shall be encrypted in transit. CONFIDENTIAL shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the business or its staff or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the business;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- Disadvantage the business in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

Information which has significant value to Screenworks Ltd, and unauthorised disclosure or dissemination would result in severe financial or reputational damage should be given the higher classification of CONFIDENTIAL.

11. Access Control Management

Physical Access

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

User Access

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

User account requests will be subject to proper justification, provisioning and an approvals process, and assigned to named individuals.

User accounts will be removed or disabled when no longer required.

Elevated or special access privileges, such as system administrator accounts, will be restricted to a limited number of authorised individuals and these access privileges will be reviewed at least quarterly.

Password Policy

Screenworks Ltd adheres to a strict password policy that must be implemented at all times. All passwords should be set to a minimum of 14 characters and contain three of the following:

a. Uppercase character
b. Lowercase character
c. Alphanumeric character between 0-9
d. Alphanumeric character (e.g. ! ” £ $ _)

Where possible, all services are subject to account lockout procedures which will restrict access to an account after 3 failed authentication attempts within a 5 minute period.

All users accounts have standard privileges matching windows user accounts.

Boundary Gateways and Firewalls

Screenworks Ltd have endeavoured to maintain boundary security through the use of a firewall, the integrity of this firewall is maintained be adhering to the following rules:

- *Internal Confidential*

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 e.g. systems or database administrators. Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

Where indicated by a risk assessment, hardware should be identified by MAC address on the network.

System Perimeter access

The boundary between the business systems and the Internet or other non-trusted networks shall be protected by a firewall, which shall be configured to meet the threat and continuously monitored.

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 and 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).

12. Computer and Network Procedures

Management

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IT Manager.

Maintenance
Systems hardware, firmware and software shall be updated in accordance with the suppliers' recommendations as approved by the IT Manager.

Patch Management
All software installed on computers and network devices is to be fully licensed and supported by the vendor.

All security patches and updates are to be applied within 14 days of release.

Accreditation
The organisation shall ensure that all new and modified information systems, applications and networks include security provisions, are correctly sized, identify the security requirements, are compatible with existing systems according to an established systems architecture (as required) and are approved by the IT Manager before they commence operation.

System Change Control
Changes to information systems, applications or networks shall be reviewed and approved by the IT Manager.

Local Data Storage
Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).

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.

13. Protection from Malicious Software

The business shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software or other active code on the organisation's property without permission from the Head of Network Security. Users breaching this requirement may be subject to disciplinary action.

All Malware Protection Software will have all engine updates applied, and this application is to be strictly adhered to.

Malware scans are be implemented using the company's anti malware software.

14. Information Security Incidents and Weaknesses

All breaches of this Policy and other information security incidents or suspected weaknesses are to be reported to the IT Manager immediately. Information

security incidents shall be logged and investigated to establish their cause and impacts with a view to avoiding similar events. If required as a result of an incident, data will be isolated to facilitate forensic examination.

15. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

16. Reporting

The IT Manager shall keep the business informed of the information security status by means of regular reports and presentations.

17. Document Revision History

This document shall be amended by releasing a new edition of the document in its entirety. The Amendment Record Sheet below records the history and issue status of this document.

Date	Author	Reason for Revision
20/04/18	Daniel Porter	Initial document
27/04/18	Daniel Porter	Revision following additional security work onsite
03/05/18	Daniel Porter	Completion of security work amendments
08/08/22	David Fox	Review and Update

Policy approved by:

Signature _____ Date _____