Pobl & Gwaith | People & Work

IT Security Policy

Version: 1.1

Author: James Hall

1. Version Control

Issue Date:	07/12/2016	Review Date:	19/12/16
Version:	1.1	Issued by:	AJC - BCC
Approved By:		Date:	
Review and consultation process			
Responsibility for Implementation and Training:			

2. 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
07/12/2016	AJC-BCC	Initial version
09/02/17	JAH-PAW	Amended version
11/04/17	JAH-PAW	Revised following ISMF

3. References

Ref #	Reference	Version
1		
2		
3		

4. Table of Contents

1. Version Control 1
2. Document Revision History 1
3. References 1
4. Table of Contents 2
5. Introduction 4
6. Objectives, Aim and Scope 4
Objectives 4
Policy Aim 4
Scope 5
7. Responsibilities 5
Implementation of the Information Security Management Forum (ISMF) 5
ISMF Terms of Reference 5
8. Legislation 6
9. Personnel Security 6
Contracts of Employment 6
Information Security Awareness Training 6
Intellectual Property Rights 6
Social Media 7
10. Asset Management 7
Asset Ownership 7
Asset Records and Management 7
Removable media 7
Removable media from external sources 7
Mobile devices (e.g. phones, tablets, laptops etc.) 7
Sensitive Information Assets 7
11. Access Control Management 8
Physical Access 8
User Access 8
Password Policy 8
Boundary Gateways and Firewalls 8
Application Access 9
Hardware Access 9
System Perimeter access 9

Monitoring System Access and Use 9

12. Computer and Network Procedures 9

Management 9

Maintenance 9

Patch Management 9

Accreditation 9

System Change Control 10

Local Data Storage 10

External Cloud Services 10

13. Protection from Malicious Software 10

14. Information Security Incidents and Weaknesses 10

15. Business Continuity and Disaster Recovery Plans 10

16. Reporting 10

5. Introduction

This IT security policy is a key component of People and Work's overall business management framework and provides the framework for the more detailed information security documentation including system level security policies, security guidance and procedures.

Failure to implement effective information security management controls can result in People and Work becoming exposed to a number of significant threats including (but not limited to):

- Malicious code entering the network;
- Hackers obtaining unauthorised access to systems and data;
- Unauthorised persons gaining access to confidential information;
- Data leakage;
- Compromise of confidentiality, integrity and availability of company sensitive data.

The adverse impacts potentially flowing from these risks include:

- Loss of availability of key systems and/or loss of data;
- Interruption of normal operations and resultant loss of revenue;
- Damage to People and Work's reputation and loss of confidence amongst clients, employees, partners and funders;
- Allegations of poor corporate governance resulting in adverse publicity and client or funder dissatisfaction;
- Confidential information falling into the hands of competitors and other third parties;
- Reputational damage to People and Work.

Compliance with these policies, procedures and standards is therefore required from all persons who have access to any of People and Work's IT infrastructure or information assets. This includes third parties (e.g. clients, partners and – in some cases – funders) as well as employees.

6. Objectives, Aim and Scope

Objectives

The objective of this Information Security Policy is to help preserve the confidentiality, integrity and availability of our 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 People and Work or supplied under contract to it.

7. Responsibilities

Ultimate responsibility for information security rests with the Director of People and Work. Employees shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the Information Risk Register and for recommending appropriate risk management measures is vested in the Director. Both the Policy and the Risk Register shall be reviewed by the Information Security Management Forum annually, or more often if appropriate and reported to the Board of Trustees annually.

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 and 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)

People and Work 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 Manager (currently, James Hall)
- Human Resources (currently, Sarah Lloyd-Jones)
- Facilities Management - BccIT
- The organisation via the Head of Research (currently, Duncan Holtom) and a Trustee.

The ISMF will:

- Define ownership and responsibility for Information Security Policy and Procedures

- Set Information Security Policy within People and Work
- Have representation on board meetings to address security issues.

8. Legislation

People and Work 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 People and Work, who may be held personally accountable for any breaches of information security for which they may be held responsible. People and Work shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- 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

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 People and Work Director. As a minimum this should include:

- Verification of identity;
- Employment history (for a minimum of the past three years);

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 People and Work's 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 annually.
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 People and Work 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 work purposes on condition that no sensitive or potentially sensitive 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 Director or IT Manager. Users breaching this requirement may be subject to disciplinary action.

10. Asset Management

Asset Ownership

Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

An accurate record of business information assets, including acquisition, ownership, modification and disposal shall be maintained. Sensitive material such as licenced software and sensitive data shall be removed from hardware before disposal.

Removable media

Official removable media shall be provided centrally and its use recorded (e.g. serial number, date, issued to, returned). Where indicated by a risk assessment, systems should be prevented from using removable media. Use of personal removable media in work information systems (e.g. USB sticks, CD, DVD and personal devices for the purposes of charging etc.) is forbidden unless approved by the IT Manager.

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 work purposes (privately or owned by People and Work) 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
- have manufacturer-supplied updates applied within 14 days of release
- be encrypted wherever possible
- be capable of being remotely tracked and wiped.

Users must inform the IT Manager or the Director immediately if the device is lost or stolen and the device must be subsequently completely wiped.

Sensitive Information Assets

People and Work shall identify particularly valuable or sensitive information assets, based upon the results of a risk assessment. The classification **SENSITIVE** 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. **SENSITIVE** shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its staff or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation ;
- 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 organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

Information which has significant value to People and Work, 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 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 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

People and Work adheres to a strict password policy that must be implemented at all times. Passwords must contain a minimum of 8 characters with uppercase and lowercase letters as well as numbers. Passwords should be changed if there is any suspicion they have been compromised.

Boundary Gateways and Firewalls

People and Work has endeavoured to maintain boundary security through the use of a firewall. The integrity of this firewall is maintained by adhering to the following rules:

- All default usernames/passwords on boundary devices have been changed and a strong password has been implemented, please see password policy statement.

- All open ports and services on each firewall have been subject to justification and approval by an appropriately qualified and authorised business representative.
- All commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOSm tftp, RPC, rlogin, rsh, rexec) have been disabled or blocked by default at the boundary firewalls.
- All firewall rules that are no longer required are to be removed or disabled in a timely manner.
- All unnecessary remote administrative interfaces have been disabled.

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 authenticated 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 by BccIT wherever practical and reviewed on a regular basis.

People & Work reserves the right to monitor 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 BccIT and 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 and BccIT.

Local Data Storage
Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly). A backup copy shall be stored in a different physical location.

External Cloud Services
Where data storage, applications or other services are provided by another organisation (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 organisation 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 IT Manager. 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.

Daily Malware scans will 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 organisation informed of the information security status by means of regular reports to the Board of Trustees.

Policy approved by:

Signature_________________________________ Date_________________