ServiceTracker Information Protection & Security Policy

Category	Information Security
Version	1.0
Classification	Public
Author	Nigel Sargent
Date	3 June 2014

Document Control

Organisation	ServiceTracker
Title	Information Protection & Security Policy
Author	Document Author – Nigel Sargent
Filename	20140603 ServiceTracker Information Security
Owner	Nigel Sargent – Co-Founder
Subject	IT Policy
Protective Marking	None
Review date	3 June 2015

Revision History

Revision Date	Version Number	Revised By	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
	Nigel Sargent	3 June 2015
	Mike Day	3 June 2015

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address / Location
Nigel Sargent	Co-Founder	nigel.sargent@servicetracker.uk.com
Mike Day	Co-Founder	mike.day@servicetracker.uk.com

Table of Contents

Policy Statement

ServiceTracker will ensure the protection of all information assets within the custody of the Business.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Purpose

Information is a major asset that ServiceTracker has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at ServiceTracker. The policy specifies the means of information handling and transfer within the Business.

Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the Organisation who have access to Information Systems or information used for ServiceTracker purposes.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Risks

ServiceTracker recognises that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents

- Inadequate destruction of data
- The loss of direct control of user access to information systems and facilities

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

Policy Compliance

If any user is found to have breached this policy, they may be subject to ServiceTracker's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the author of this document.

Policy Governance

The following table identifies who within ServiceTracker is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment, all employees, all temporary staff, all contractors etc.

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by Nigel Sargent

References

The following ServiceTracker policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.

- Remote Working Policy.
- Removable Media Policy.

The following ServiceTracker policy documents are indirectly relevant to this policy:

- ServiceTracker Information Sensitivity Policy.
- ServiceTracker Risk Assessment Policy.
- ServiceTracker Ethics Policy.

Key Messages

- The Business must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF).
- Information up to RESTRICTED sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until the Information Security Officer is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- PROTECT and RESTRICTED information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing PROTECT or RESTRICTED classified information to any external organisation is also prohibited, unless via the GCSx email.
- Where GCSx email is available to connect the sender and receiver of the email message, this must be used for all external email use and must be used for communicating PROTECT or RESTRICTED material.
- The disclosure of PROTECT or RESTRICTED classified information in any way other than via GCSx email is a disciplinary offence.

Appendix 1

A1 Applying the Policy

A1.1 Information Asset Management

A1.1.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

ServiceTracker must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

A1.1.2 Classifying Information

On creation, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled in accordance with the HMG Security Policy Framework (SPF). The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification. Information up to RESTRICTED sent via GCSx must be labelled appropriately using the SPF guidance.

The SPF requires information assets to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependent on this scheme.

The classes are:

- Unclassified (Sometimes labelled Not Protectively Marked).
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.

- TOP SECRET.

You should refer to the local GPMS usage guide for full details on the application of information classification.

Personal Information

Personal information is any information about any living, identifiable individual. The business is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998. Details of specific requirements can be found in the Legal Responsibilities Policy.

A1.1.3 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

A1.1.4 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

A1.1.5 Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spread sheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

A1.1.6 Corporate Information Assets

For information assets whose use throughout the organisation is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

A1.1.7 Acceptable Use of Information Assets

The Council must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to all ServiceTracker Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the business and use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

As a minimum this will include:

- Email Policy.
- Internet Acceptable Usage Policy.
- Computer and Telephone Misuse Policy.
- Software Policy.
- Remote Working Policy.
- Removable Media Policy.

A1.2 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Records management and retention guidance will be followed .

Staff should not be allowed to access information until the line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

Databases holding personal information will have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information.

Files which are identified as a potential security risk should only be stored on secure network areas e.g. ESCR.

A1.3 Disclosure of Information

A1.3.1 Sharing PROTECT or RESTRICTED Information with other Organisations

PROTECT or RESTRICTED information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

Disclosing PROTECT or RESTRICTED information to any external organisation is also **prohibited**, unless via the Government Connect Secure Extranet (GCSx) email. Emails sent between gov.uk addresses are held within the same network and are deemed to be secure. However, emails sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT and RESTRICTED material. For further information see the Email Policy.

An official email legal disclaimer must be contained with any email sent.

The disclosure of PROTECT or RESTRICTED information in any way other than via GCSx email is a disciplinary offence. If there is suspicion of an board member or employee treating PROTECT or RESTRICTED information in a way that could be harmful to HMG's interests, the Organisation, or to the data subject and the person may be subject to disciplinary procedure.

Any sharing or transfer of Council information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

END OF DOCUMENT

Information Protection Policy