# Information Security Policy Suite

## Information Governance and Security Policy

## ISPS - 001

This policy is available in alternative formats upon request, such as large print or electronically. Please contact the Technology Services Management Team, to obtain a copy in a different format.



Approval Authority: {insert approval body here} Approval Date: xx/xx/2012

## Preface

This policy is part of the Information Security Policy Suite and should be read in conjunction with these as well as any other policies, standards, guidelines and procedures that Horsham District Council may introduce.

## Definitions

'The Council' is Horsham District Council.

'Information' is any data held by the Horsham District Council whether it is held in electronic or paper format.

Please see the separate document 'Glossary of Terms' for definitions of terms that are used throughout the Information Security Policy Suite.

# Policy Contents

1. Purpose ..... 4
1.1 Objective ..... 4
2. Scope ..... 4
3. Policy Statement ..... 5
4. Responsibilities ..... 6
4.1 Senior Management ..... 6
4.2 Senior Information Risk Owner (SIRO) ..... 6
4.2.1 The Council's SIRO ..... 6
4.2.2 The SIRO of Horsham District Council ..... 7
4.2.3 The SIRO of Mid Sussex District Council ..... 7
4.3 Information Security Manager (ISM) – in conjunction with other delegated officers ..... 7
4.3.1 Information Security Incident Management Specific ..... 8
4.4 Information Asset Owners (IAOs) ..... 8
4.4.1 Information Security Incident Management specific ..... 8
4.5 All Other Managers and Supervisors ..... 8
4.6 Everyone ..... 9
5. Training associated with this Policy ..... 9
6. Monitoring ..... 9
6.1 Non-compliance ..... 9
6.2 Review ..... 10
7. Equality Impact Assessment (EIA) ..... 10
8. Related documents ..... 10
Appendix A: Relevant Legislation ..... 12
Appendix B: Exception Handling Procedure ..... 12

# 1. Purpose

The Council recognises and accepts that there are risks associated with people accessing and handling information to conduct official Council business. We need to be aware of vulnerabilities that could be exploited and guard information from potential threats.[1]

The Council is committed to implementing controls to prevent the unauthorised access, interference, misuse, disclosure, loss or theft, of the Council's information, so far as is reasonably practicable.

This document sets out the policy of the Horsham District Council regarding the security of their information assets to guarantee the confidentiality, integrity and availability of Council information and systems, so that sensitive information is protected from unauthorised disclosure, the accuracy and completeness of that information is safeguarded, and the information is available to staff, members, and third parties when required.

Effective information management will bring many benefits to the Council by facilitating and supporting more efficient working, better decision making, improved customer service and business transformation.

## 1.1 Objective

The objective of the Information Security Policy Suite is to foster trust with our customers and partners and to ensure that we uphold the rights of individuals with regard to the information we hold. Full compliance with the Information Security Policy Suite will help us to manage the risk from all information security threats.

# 2. Scope

This policy applies to anyone working with information or information systems controlled by Horsham District Council including Officers, Members, partners, contractors and any other third parties.

This policy applies to all information held, created, modified or accessed from the effective date of this policy. It includes information in any form, no matter whether it is stationary (i.e. at rest, e.g. an electronic or paper document) or in transit, e.g. file transfer, e-mail, fax, phone, post, courier). It also covers the buildings, premises and systems which contain that information (refer to the Building, Infrastructure and Equipment Security Policy).



[1] These are managed through the Council's Information Security Risk Management policy with the potential for significant risks to be escalated to the Council's Corporate Risk Register.

## 3. Policy Statement

The Council will:

a. Ensure that it allocates the roles of SIRO, ISM and IAOs to teams or role profiles within the council.

b. Ensure that it complies with relevant UK and EU information management legislation[2] and standards including (but not limited to):

   b.1. Data Protection Act 1998; (Data Protection Act 2018)

   b.2. Freedom of Information Act 2005;

   b.3. Privacy and Electronic Communications (EC Directive) Regulations 2003;

   b.4. Payment Card Industry Data Security Standard (PCI DSS);

   b.5. Government sponsored Codes of Connection, e.g. PSN.

c. Uphold the legal rights of any person to confidentiality, and ensure that information about them is used and shared legitimately;

d. Ensure that it actively publishes a wide range of relevant and appropriate information to the public;

e. Ensure that personal and sensitive personal data is securely stored, handled and shared appropriately (see the Business Information Sharing (ISPS-008) and Information Handling (ISPS-009) Policies);

f. Provide information to applicants within the relevant legislative timelines where they have a right to it, and where it is not already published;

g. Ensure that any third parties have adequate procedures in place for the secure and compliant handling of the Council's information assets;

h. Maintain the accuracy and completeness of its information assets;

i. Ensure that information security risks are identified and assessed and that appropriate controls are put in place where necessary;

j. Ensure that all Information security incidents, actual or suspected, are reported and managed in accordance with the Council's Incident Management guidelines and procedures.

k. Ensure that appropriate Business Continuity and Disaster Recovery incident response plans are in place for all identified business critical and sensitive information and systems;

l. Require anyone with access to its information and systems to comply with the Council's Information Security Policy Suite and any standards, guidelines and procedures;

m. Promote awareness of the requirements of Information Governance and provide appropriate training for its staff and Members;

[2] See Appendix A on page 12 for a list of the current information management focused legislation.

n. Take appropriate action against anyone found to be in breach of one of the policies that form the Information Security Policy Suite.

# 4. Responsibilities

The implementation of the Information Security Policy Suite emphasises the Council's view that the protection of Council assets is a primary management responsibility and must be approached as such.

The responsibilities listed below apply to each policy in the Information Security Policy Suite. Section 4 of each policy specifies any additional responsibilities that may apply.

## 4.1 Senior Management

The overall responsibility for Information Governance and Security lies with the Senior Information Risk Owner (SIRO) and is administered through the Corporate Governance group. Their responsibilities include:

a. Being responsible for the formulation and implementation of the Information Governance and Security Policy and the other policies in the Information Security Policy Suite.

b. Being accountable to the elected Members for the overall implementation of all matters relating to this Information Governance and Security Policy and the other policies in the Information Security Policy Suite.

c. The Senior Information Risk Owner (SIRO) is responsible for ensuring the implementation and compliance with the Information Security Policy Suite and any supporting standards, guidelines and procedures within the Council.

## 4.2 Senior Information Risk Owner (SIRO)

### 4.2.1 The Council's SIRO

The Council's SIRO, the Director of Corporate Resources, shall be responsible for information security within the Council in accordance with the Information Security Policy Suite. Their responsibilities include:

a. To ensure that all current developments in security practices are in place and monitor the revision of the Information Security Policy Suite and any supporting standards, guidelines and procedures as required;

b. Delegating as required the authority to monitor compliance with the Information Security Policy Suite to such officer(s) as deemed fit to discharge such a function,;

c. Ensuring that information governance is embedded into the organisation;

d. Ensuring that potential risks to corporate information are mitigated;

e. Ensuring that resources are available to provide such protective measures as may be appropriate to meet security requirements, e.g. finance, people, etc.

f. Chairing the Information Security Post Incident Review (only where the incident was classified with an impact of medium or high);

g. Following the Council's agreed Exception Procedure if an exception to this policy is required (example procedure provided in Appendix B on page 12).

## 4.3 Information Security Officer (ISO) – In lieu of this role, this function is fulfilled by the Technology Services Management Team

The ISO shall be responsible to the SIRO for the discharge of the following on a day-to-day basis with regard to the Information Security Policy Suite. Their responsibilities include:

a. Developing, monitoring and overseeing the implementation of the Information Security Policy Suite and any associated standards, guidelines and procedures;

b. Ensuring that all staff and Members are aware of the information security policies, standards, guidelines and procedures and where necessary ensure that the Council provides instruction and training in security matters;

c. Advising and consulting with Heads of Service as necessary where losses arise and implementing agreed procedures to reduce or eliminate loss;

d. Identifying security risks to the Council's information assets and introducing appropriate controls to mitigate these;

e. Ensuring that all aspects of security are constantly reviewed and, where appropriate, ensuring that the SIRO is aware of any security breaches that may occur;

f. Maintaining appropriate records of all matters relating to information security within the Council.

### 4.3.1 Information Security Incident Management Specific

g. Creating and co-ordinating the Security Incident Response Team for incidents with a medium or high impact;

h. Maintaining records of security incidents and actions taken;

i. Co-ordinating the Post Incident Review (only where the incident was classified with an impact of medium or high);

## 4.4 Heads of Service

Heads of Service shall be responsible to their respective line managers for the implementation of controls supporting the Information Security Policy Suite and any standards, guidelines and procedures within their own areas of responsibility. Their responsibilities include:

a. Being responsible for information asset management in their departments;

b. Ensuring adequate supervision, information and necessary training for staff and / or Members such that their responsibilities are fully understood and performed;

c. Ensuring that all information assets have been risk assessed and classified in accordance with the Information Security Risk Management Guidelines.

d. Implementing appropriate security controls to mitigate these in consultation with the ISO;

e. Ensuring compliance by all staff, including temporary and casual staff as well as Members and contractors that handle their information assets.

### 4.4.1 Information Security Incident Management specific

f. Responding to information security incidents relating to their information assets;

g. Co-ordinating the response to the security incident ensuring that appropriate actions are taken;

h. Participation on a Security Incident Response Team if invited to do so;

i. Contributing to the Post Incident Review (only where the incident was classified with an impact of medium or high).

## 4.5 All Other Managers

Will be responsible to their line manager for implementation of controls supporting the Information Security Policy Suite and any standards, guidelines and procedures within their own areas of responsibility. Their responsibilities include:

a. Ensuring that all staff under their supervision are aware of the security procedures and their obligation in respect of them;

b. Ensuring that any non-conformance with the Information Security Policy Suite is subjected to appropriate action in accordance with the Council's disciplinary procedures;

c. Ensuring that potential or actual information security incidents are reported in accordance with the Information Security Incident Management Policy;

d. Undertaking information security risk assessments to identify practices that pose a threat to the security of the Council's information assets and notifying the Heads Of Service;

e. Consulting and co-operating with the Heads of Service and any other designated officers and managers to achieve information security both in and out of the workplace.

## 4.6 Everyone

Shall be directly accountable for compliance with the Information Security Policy Suite, standards, guidelines and procedures. Their responsibilities include:

a. Ensuring that they participate in and complete any training and awareness provided by the Council within requested time scales in order to support compliance with the Information Security Policy Suite and any standards, guidelines and procedures;

b. Advising their line manager (or democratic services for Members) of any matters that they consider might pose a threat to the security of premises, health and safety of staff or information security;

c. Promptly reporting on actual or potential information security incidents in accordance with the Information Security Incident Management Policy;

d. Assisting with the investigation of any losses by internal or external sources;

e. Seeking advice from the IAO or ISO when uncertain about something relating to information security.

# 5. Training associated with this Policy

As part of the Council's on-going commitment to implementing and further developing the Information Security Policy Suite, it is committed to regularly educating, training and raising awareness of staff and members on the policy statements, their responsibilities and any further commitments required by the Council to adhere to legislation.

If anyone requires support, advice or guidance on any element outlined in this policy they should speak with their line manager.

# 6. Monitoring

Compliance with the Information Security Policy Suite and its associated standards, guidelines and procedures will be monitored through the Council's management structure.

## 6.1 Non-compliance

All the policies and standards that form part of the Information Security Policy Suite must be complied with fully by all staff, Members, contractors and any other persons handling the Council's information assets.

Appropriate action will be taken under the Council's Disciplinary Process for non-compliance.

If anyone does not understand the implications of this policy or how it may apply to them, they should seek advice from their Line Manager.

## 6.2 Review

All policies including this policy will be reviewed on an annual basis to take account of one or any of the following:

- Legislative or regulatory changes;
- Structural or role changes;
- Operational or technological changes;
- Organisational learning;
- Audits and reviews of the effectiveness of the policy.

It may also be supplemented to deal with any special contingency which may give rise to perceived or specific security issues.

## 7. Equality Impact Assessment (EIA)

An equality impact assessment has been completed for all the policies that form part of the Information Security Policy Suite.

## 8. Related documents

This policy should be read in conjunction with the following documents that form the Information Security Policy Suite;

- ISPS-002 Acceptable Use;
- ISPS-003 Remote working;
- ISPS-004 Building, Infrastructure and Equipment Security;
- ISPS-005 ICT Security;
- ISPS-006 Access Control (includes Remote Access and Supplier Access policies);
- ISPS-007 Backup, Restore and Recovery;
- ISPS-008 Business Data (Information) Sharing;
- ISPS-009 Information Handling (includes Clear Desk, Removable Media and Protective Marking Policies);
- ISPS-010 Records Management;
- ISPS-011 Data Protection (DPA);
- ISPS-012 Freedom of Information and Environmental Information Regulations;
- Any supporting standards, guidelines and procedures.

# Appendix A: Relevant Legislation

a. This includes but is not limited to the Computers Misuse Act 1990 and the
b. Data Protection Act 1998; Data Protection Act 2018.

# Appendix B: Exception Handling Procedure

a. Any exceptions to any policy in the Information Security Policy Suite should be documented in writing
b. This should summarise:
    b.1. The circumstances giving rise to the exception;
    b.2. The rationale for granting it;
    b.3. Acknowledgement that they are accepting the risk on behalf of the Council.
c. If this relates to an ICT security control a copy of this 'Risk Acceptance Confirmation' should be sent to:
    c.1. The Technology Services Management Team who are responsible for implementing any actions arising from it;
    c.2. The Technology Services Management Team of Horsham District Council who is responsible for retaining it and updating the operational information security risk register;
    c.3. The SIRO of Horsham District Council for information.