Monitoring in place	**9**
Monitoring not in place	**25**

Protective Monitoring Risk Assessment

Risk Assessment

Area covered by this assessment	**Monitoring activity on the network, particularly at the gateway in order to detect and prevent potential security incidents whether these are technical attacks or abuses of business.**

Activity requiring assessment and requestor	**Requested by the business as part of the Privacy Impact Assessment covering Protective Monitoring** **Technical detail** Protective monitoring is an essential component of risk management. Various legislation and codes of practice including the Data Protection Act 1998, and ISO 27001/2 Information Security Management Systems impose a duty on Aberdeen City Council to protect its information assets and to provide the assurances that appropriate controls are in place. It is recommended in a number of regulatory and industry best practices, such as the Payment Card Industry Data Security Standard (PCI DSS) and Cyber Security Essentials. It is also a requirement for connection to the Public Services Network (PSN). This assessment covers the monitoring and auditing of staff activity as a means of ensuring information security and ensuring that all staff comply with Council Policies and Procedures and the standards of behaviour expected by Aberdeen City Council. **Related Policy Document Suite** Policy and Strategy • ICT Acceptable Use Policy • Employee Code of Conduct • Councillor Code of Conduct • Protective Monitoring Policy (Hyperlink when on the Zone) Procedures • Access to Information Procedure (Hyperlink when on the Zone) Assessments • Protective Monitoring Privacy Impact Assessment (Hyperlink when on the Zone) **Related Legislation and Supporting Documents** Acts • The Data Protection Act (1998) Requires that processing of personal data is done so lawfully and fairly, is used for limited specifically stated purposes and used in way that is adequate, relevant and not excessive. • General Data Protection Regulation From 25th May 2018, this replaces the Data Protection Act (1998) and requires the Council to process personal data lawfully, fairly and transparently, and requires the Council to secure the personal data it

holds. The GDPR is designed to enable individuals to better control their personal data. Penalties for breaches are more severe than under the 1998 Act.

- The Computer Misuse Act (1990)
  Disallows unauthorised access or acts in relation to computer systems, data or materials.

- The Copyright, Designs and Patents Act (1988)
  Protects the rights of creators to control the ways in which their materials are used. There is a duty on the Council to prevent breaches of Copyright.

- The Health & Safety at Work Act (1974)
  Protects the health, including mental health of their employees.

- The Human Rights Act (1998)
  The right to respect for family and private life, home and correspondence. This right is not absolute and must be balanced with the need of the Council to protect its information.

- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000 (LBPR).
  Allows interception of communications by businesses on their own telecommunications networks, for instance, to detect employee-mail abuse or to record telephone conversations to evidence transactions.

Related Standards

- ISO27001/2
  A framework of policies and procedures that includes all legal, physical and technical controls.

- PSN
  A public services shared information and communications infrastructure for which we need to remain compliant.

Regulations

- PCI DSS
  The Council is required to meet this standard in order to take card payments.

Best Practice Guides

- National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13)
  Provides advice on good practice to help meet Protective Monitoring obligations.

- Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work.
- Aims to strike a balance between the legitimate expectations of workers and the legitimate interests of employers.

Assessor	**Norman Hogg** **(Security Architect)**	Date of assessment	**25/09/17**	Date of reassessment	

Existing safety measures and assets at risk.	**Existing Measures:** This assessment is measured against the impact on individual rights and the risk to the business based on existing controls in place (which will include Protective Monitoring Policy, Protective Monitoring Privacy Impact Assessment and Access to Information Procedure when approved) ***to be removed from document once approved*** **Assets at risk:** Data. Corporate network. Reputation. Individual Rights.

Approver Signature>	**Steven Robertson** **(SIRO)** *****	Date of approval/ rejection	**XX/XX/17**	Date of re-approval	

Decision	**Accept assessment**	
	Reject assessment	

SCORING SYSTEM

Severity	Likelihood of occurrence
5 = Very high	5 = Very high
4 = High	4 = Likely
3 = Moderate	3 = Quite possible
2 = Slight	2 = Possible
1 = Nil	1 = Not likely

Risk rating = Severity x Likelihood.

>10 requires risk acceptance, risk reduction, risk avoidance, risk transference.

Hazard Type

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**
1. Monitoring is excessive as most activity is recorded. Risk of accessing personal information.	4	2	8	1	3	2	6	15
2. Violation of rights and liberties. Risk of breaching legislation.	4	2	8	25	3	2	6	25
3. Monitoring is intrusive. Prevents staff performing duties, mistrust.	3	2	6	1	3	2	6	1
4. Passwords and other Personal information may be captured.	3	2	6	20	3	2	6	20
5. Staff are unaware of policy or procedure.	3	3	9	25	3	3	9	25
6. Policy and procedure are inadequate.	4	2	6	25	4	2	8	25
7. Access to logged information is not controlled.	4	2	8	1	4	2	8	20
8. False positive information leads to investigation.	3	2	6	1	3	2	6	16
9. Inability to perform job functions due to Emails or Internet sites being blocked.	2	2	4	1	2	2	4	25

PROPOSED ACTION

In order to ensure appropriate risks and mitigations were identified for this document, consultation and review took place as follows:

Security Architect
Performance and Risk Manager
Infrastructure Architect
Security Analyst x 2
HR Team Leader
Solicitor
Best practice guides
Web Resources
Government Guidelines

Results of Analysis:

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**
1. Monitoring is excessive as most activity is recorded. Risk of accessing personal information.	4	2	8	1	3	2	6	15

'The Data Protection Act does not prevent employers from monitoring workers, but where monitoring involves the collection, storage and use of personal information, it must be neither routine nor excessive'

In order to protect both the organisation and the individual it is important that we have both comprehensive and accurate records. Without these records assumptions rather than conclusions can be drawn and evidence of actual facts will be minimal. Without adequate records the business may breach legislation.

Monitoring significantly reduces the risk of the businesses information being compromised.

Please reference the '*Protective Monitoring Privacy Impact Assessment*' (Hyperlink when on Zone) – 'Scope of Monitoring', 'Alternatives to Monitoring' and 'Justification for Monitoring sections'.

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**
2. Violation of rights and liberties. Risk of breaching legislation.	4	2	8	25	3	2	6	25

PROPOSED ACTION

A balance must be found between what is monitored and the rights of the individual. To this end:

The majority of monitoring and threat prevention is automated by technology and detailed information is not viewed.

Although certain activities are logged these would only be accessed as part of an investigation.

Where information does have to be viewed it is done so in a controlled manor and only to the level required.

The two main areas where such visibility may take place are with Internet traffic and Email.

Internet traffic: Blocks are in force against sites that are identified as high risk, reports are generated which show attempted access to those sites. Patterns or excessive activity can indicate an infected device, a compromised device or deliberate action by an individual to bypass security measures. In the case of the individual, only where such activity is significantly out of the ordinary and with documented authority will any further investigation take place.

Email: Email containing certain attachments such as executables or compressed Zip files will be quarantined. These are key routes for compromise as they often contain hidden malware. Manual intervention is required before releasing to the recipient.

Monitoring significantly reduces the risk of an individual's information being compromised.
Monitoring significantly reduces the risk of the businesses information being compromised.

Please reference the '*Protective Monitoring Privacy Impact Assessment*' (Hyperlink when on Zone) – 'Scope of Monitoring', 'Justification for Monitoring sections'.

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**
3. Monitoring is intrusive. Prevents staff performing duties, mistrust.	3	2	6	1	3	2	6	1

Monitoring is only mildly intrusive. It is transparent to the end user most of the time and normally only becomes apparent when an individual is blocked from accessing a website.
There is no risk associated with this hazard if we do not monitor.

Monitoring adds a low risk for both individuals and the business.

Please reference the '*Protective Monitoring Privacy Impact Assessment*' (Hyperlink when on Zone) – 'Scope of Monitoring', 'Justification for Monitoring sections'.

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			

PROPOSED ACTION

Hazard Type	Severity	Likelihood	Risk Rating	Without Monitoring	Severity	Likelihood	Risk Rating	Without Monitoring
4. Passwords and other Personal information may be captured.	3	2	6	20	3	2	6	20

Protective Monitoring protects both the business and the individual. Passwords and Personal Information are never targeted for capture, however if such information is sent externally, unencrypted in an Email the Email system will hold a copy unless it is deleted from the senders 'Sent Items' folder.

Protective Monitoring plays a major role in preventing an individual from inadvertently giving such information to a fraudulent actor. For example:

- Many spam and phishing emails are prevented from entering the organisation.
- Individuals are prevented from accessing known websites which are fraudulent, contain malware or that have been compromised.
- Where an individual clicks a fraudulent link or file in an Email, protection measures help prevent the link activating or the file being run.

Monitoring significantly reduces the risk of an individual's information being compromised.
Monitoring significantly reduces the risk of the businesses information being compromised.

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	Severity	Likelihood	Risk Rating	Without Monitoring	Severity	Likelihood	Risk Rating	Without Monitoring
5. Staff are unaware of policy or procedure.	3	3	9	25	3	3	9	25

The following documents will be available on the Zone:

- ICT Acceptable Use Policy (Hyperlink when on Zone)
- Protective Monitoring Policy (Hyperlink when on Zone)
- Protective Monitoring Privacy Impact Assessment (Hyperlink when on Zone)
- Protective Monitoring Risk Assessment
- Access to Information Procedure (Hyperlink when on Zone)
- Access to Information Form (Hyperlink when on Zone)

In addition:

- All staff with management responsibility will be advised of the Access to Information Procedure.
- All IT staff will be advised of the Access to Information Procedure.

There are many policies and procedures in use across the business and it is unrealistic to believe that everyone will know all the policies and procedures. Everyone should know however where to find them when they need to reference them.

PROPOSED ACTION
Policies and Procedures significantly reduce the risk of an individual's information being compromised. Policies and Procedures significantly reduce the risk of the businesses information being compromised.

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**
6. Policy and procedure are inadequate.	4	2	6	25	4	2	8	25

It is an almost impossible task to have Policy, Procedure and Assessments that document all conceivable eventualities. Such documents need to be able to cover the majority of circumstances but should not be considered as all-encompassing.

The Protective Monitoring suite of documents have had input from and been reviewed by:

- IT and Transformation
- Human Resources and Customer Service
- Legal and Democratic Services
- Unions
- Aberdeen City Council Finance, Policy and Resources Committee

Policies and Procedures significantly reduce the risk of an individual's information being compromised.
Policies and Procedures significantly reduce the risk of the businesses information being compromised.

	Risk to Individuals if Monitoring In place				Risk to Business if Monitoring In place			
Hazard Type	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**	**Severity**	**Likelihood**	**Risk Rating**	**Without Monitoring**
7. Access to logged information is not controlled.	4	2	8	1	4	2	8	20

Access to such information is restricted to key staff. Access cannot be obtained via standard user accounts and requires authenticated administrative privileges. Out with this, if information is requested due to a security incident or as part of an investigation then the 'Access to Information Procedure' (Hyperlink when on Zone) shall apply.

Logging/Auditing of administrator access is in place.

Monitoring significantly reduces the risk of the businesses information being compromised.

PROPOSED ACTION

Hazard Type	Risk to Individuals if Monitoring In place: Severity	Likelihood	Risk Rating	Without Monitoring	Risk to Business if Monitoring In place: Severity	Likelihood	Risk Rating	Without Monitoring
8. False positive information leads to investigation.	3	2	6	1	3	2	6	16

Most of the monitoring and preventative measures are automatic and in the majority of cases detail is never seen by human eyes. High level trending statistics may be generated for inclusion in reports.

Where our systems do flag up activity of potential concern these are in most cases not due to activity by individuals.

In the course of their duties, Security Analysts may come across patterns of traffic or information that requires further analysis. A high level but focussed look at the patterns may take place and may identify individuals. In most cases the activity is either not due to the individual or is not deliberate or persistent activity by the individual and requires no further investigation.

Where it is deemed further investigation is required the 'Access to Information Procedure' (Hyperlink when on Zone) will be followed.

There is significant risk to the business of instigating false investigations if we did not have the evidence to back up any claims.

Hazard Type	Risk to Individuals if Monitoring In place: Severity	Likelihood	Risk Rating	Without Monitoring	Risk to Business if Monitoring In place: Severity	Likelihood	Risk Rating	Without Monitoring
9. Inability to perform job functions due to Emails or Internet sites being blocked.	2	2	4	1	2	2	4	25

The blocking of Email or Internet sites should not have an impact on job functions. These are blocked due to the risk they pose to the business or the individual and could have a major impact on the job function if not blocked. Where a particular job role requires that a normally blocked site be open then this can be accommodated on a per user basis where there is a business case and with authorisation.

There is significant risk to the business if restrictions are not put in place.

PROPOSED ACTION