CORPORATE POLICY

PROTECTIVE MONITORING

Date Created:	October 2017	
Version:	V1.1	
Location:		
Author (s) of Document:	Norman Hogg, Security Architect	
Approval Authority	Audit Risk & Scrutiny Committee	
Scheduled Review:	October 2018	
Changes:	Month YYYY	Brief description of changes

What is this policy for?

This policy defines how Aberdeen City Council aims to detect and prevent potential security incidents, whether technical attacks or abuses of business process. This policy does not describe specific events collected but documents the requirements for collection and analysis in relation to protective monitoring and intrusion detection.

Who is this policy for?

This policy applies to all staff, agency staff, elected members, contractors and sub-contractors, and to any person, without exception, who uses or requires access to the Aberdeen City Council Information Technology, Data Assets or associated Infrastructure.

Why do we need this policy?

Protective monitoring is an essential component of risk management. Various pieces of legislation and codes of practice, including the Data Protection Act (1998), and ISO 27001/2 Standards for Information Security Management Systems, impose a duty on Aberdeen City Council to protect its information assets and 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) that such a policy exists.

Protective monitoring underpins the Shaping Aberdeen Corporate vision by aiming to protect the data that has been entrusted to us by our customers.

What does it mean for the Council? (Policy Statement)

Monitoring, includes the routine supervision of performance and staff behaviour in line with the Employee Code of Conduct (Hyperlink when on Zone). This extends to the use by staff of IT equipment or infrastructure provided by the organisation for business purposes.

Protective Monitoring is a lawful and ethical practice used to assist Aberdeen City Council in the protection of all users, assets and information and to assist in the investigation of misconduct or criminal activity. As such the audit systems may monitor and record all computer based actions conducted using any piece Aberdeen City Council IT equipment or infrastructure.

This policy defines the monitoring and auditing of activity to ensure all compliance with Council Policies and Procedures, and with the standards of behaviour expected by Aberdeen City Council and the public.

This policy does not over-ride any existing policies nor negate any existing guidance regarding information security, data protection or acceptable use. It supplements such policies but with a specific focus on the protective monitoring of the Aberdeen City Council network, and the data held within or transported by it.

The main aims and objectives are:

- To ensure the data integrity of the information held.
- To enhance operational security.
- To identify misuse.
- To monitor exceptional usage.

- To support intelligence led investigations.
- To protect the Council by providing the Fraud Team the means by which they can effectively seek out those who abuse their position for personal gain or benefit of others.
- To protect Council information and assets from malicious or accidental disclosure

All users must note that the monitoring will include any personal use staff make of Council computer equipment or infrastructure, even if undertaken in their own time.

How will we make it happen?

PROTECTIVE MONITORING CONTROLS
The implementation of protective monitoring for the Aberdeen City Council network has been aligned to the requirements of the National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13), as recommended by the UK government. It also aligns with the Information Commissioner's Employment Practices Code, Part 3: Monitoring at Work.

Aberdeen City Council shall implement Protective Monitoring Controls (PMCs) in accordance with the guidance documented in the GPG 13. The PMCs are summarised below and detailed further in Appendix I (see page 5):

- PMC1 Accurate time in logs
- PMC2 Recording relating to business traffic crossing a boundary
- PMC3 Recording relating to suspicious activity at a boundary
- PMC4 Recording of workstation, server or device status
- PMC5 Recording relating to suspicious internal network activity
- PMC6 Recording relating to network connections
- PMC7 Recording of session activity by user and workstation
- PMC8 Recording of data backup status
- PMC9 Alerting critical events
- PMC10 Reporting on the status of the audit system
- PMC11 Production of sanitised and statistical management reports
- PMC12 Providing a legal framework for Protective Monitoring activities

How will we know if it's working?

Statistics are gathered by the Security Architect and provided in the quarterly Information Governance Report. These statistics show the level of identified threat and the number of incidents of significance. A rise in the level of incidents may indicate the solutions are not working, in which case further investigations will be carried out.

How will we manage any risks that affect this policy?

IT Risk Register
The risks to the Council from a failure to perform adequate Protective Monitoring are outlined in the Corporate Governance IT Risk Register, which is managed by the Council's Senior Information Risk Owner (SIRO). This Register is used to document known IT risks of significance and to ensure that the measures and actions identified are controlled and mitigated. See Protective Monitoring Risk Assessment (Hyperlink when on Zone)

Service Risk Registers
Information Asset Owners are responsible for managing risk to the information assets that they are responsible for, these risks are managed through Service Risk Registers and included in Business Continuity planning and disaster recovery arrangements wherever appropriate.

Strategic Risk Register

Information management and security also pose a strategic risk for the Council and this is recorded in the Strategic Risk Register. The SIRO provides the Council's Corporate Management Team with regular updates on the strength of controls in place against this risk.

How will we make sure this policy is kept up to date?

This policy will be reviewed annually by the Council's Security Architect to ensure that it meets requirements of the business, accountability and standards of best practice.

Related Policy Document Suite

Policy and Strategy

- ICT Acceptable Use Policy
- Employee Code of Conduct
- Councillor Code of Conduct

Procedures

- Access to Information Procedure (Hyperlink when on the Zone)

Assessments

- Protective Monitoring Privacy Impact Assessment (Hyperlink when on the Zone)
- Protective Monitoring Risk 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.

Appendix I

PMC1 – Accurate Time in Logs

Control Description:

- Provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitate collation of events between those components.

Aberdeen City Council Control Process in Place:

- Core network components and monitoring devices are synchronised using the Network Time protocol (NTP). This protocol provides a means of synchronizing to a globally referenced time source.

PMC2 – Recording Relating to Business Traffic Crossing a Boundary

Control Description:

- To provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.

Aberdeen City Council Control Process in Place:

- Detection of Malware which is then blocked, logged and reported on. Further analysis of logs may take place for specific incidents, to identify trends or as part of an investigation. This data may include information which will identify individuals who have had malware sent to them, whose device is malware infected or have visited websites infected with malware.

- All Internet browsing is routinely logged. An individual's browsing activity is generally anonymous. We do not interrogate activity unless instructed to as part of an investigation and through the Access to Information Procedure. (Hyperlink when on Zone)

- We regularly run reports for security purposes. These reports may identify individuals deliberately or inadvertently putting the organisation at risk or attempting to circumvent Aberdeen City Councils security measures. Any significant identified behaviour will be reported to management. Further investigation will only take place on instruction as part of an investigation and through the Access to Information Procedure. (Hyperlink when on Zone).

- Imported content may be blocked. Certain file types may be quarantined for further analysis before being let into the organisation or may be rejected outright.

- Exported content may be blocked. Certain file types may be quarantined for further analysis before being allowed to leave the organisation or may be rejected outright. Automatic file scanning for Data Loss Prevention may also quarantine a file.

PMC3 – Recording Relating to Suspicious Behavior at a Boundary

Control Description:

- To provide reports, monitoring, recording and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour.

Aberdeen City Council Control Process in Place:

- Next Generation Firewalls employ threat identification and prevention mechanisms. All 'events' and 'threats' identified by the firewalls are logged, blocked and correlated. Regular high level reports are run on these to identify particular issues or incidents and to provide trending statistics. Along with correlated events these may indicate an infected or compromised machine or system, an individual putting Aberdeen City Council or themselves at risk, or individuals, whether internal or external, attempting to circumvent Aberdeen City Councils security measures.

- Routers direct the flow of traffic within the organisation and into and out of the organisation and provide secure separation at the network boundaries.

- Switches direct the flow of traffic within the organisation and provide a level of secure boundary separation.

PMC4 – Recording of Workstation, Server or Device Status

Control Description:

- To detect changes to device status and configuration.

Aberdeen City Council Control Process in Place:

- Monitoring:

    - A tool called 'System Centre Configuration Manager' (SCCM), regularly checks devices for installed software. This is a key security measure as any unpatched software poses a security risk. This system will also apply patches to any Microsoft software on devices.

- The status of Anti-Virus software on devices is monitored centrally to ensure devices are being updated with new definitions, to gather information on any infections or attempted infections and to remotely roll out updates.

PMC5 – Recording Relating to Suspicious Internal Network Activity

Control Description:

- To monitor critical boundaries and resources within internal networks to detect suspicious activity either by internal users or by external attackers that may indicate attacks, pre-cursor to attacks or breach of regulations or compliance.

- Likely boundaries and resources may include but are not limited to:

    - Core messaging infrastructure (e.g. email servers and directory servers).
    - Sensitive databases (e.g. HR databases, finance, procurement/contracts, etc).
    - Information exchanges with third parties.

Aberdeen City Council Control Process in Place:

- Monitoring:

    - Data traffic levels across the organisation are monitored. Deviations from normal can indicate suspicious activity.

    - Status and performance of infrastructure equipment across the organisation is monitored. Changes can indicate suspicious activity.

    - Firewalls are monitored for changes to their status or deviations from normal activity.

  - Specialist Packet Sniffing technology may be deployed.
  - Endpoint Security mechanisms monitor critical resources.
  - Anti-Virus is installed on servers and Internet facing Firewalls.
  - Core servers are monitored with various protections in place with an aim to detect and prevent unauthorised change.

- Logging:
  - System logs indicating both successful and unsuccessful logins are recorded within some systems.
  - Logging of all Emails sent or received takes place (not the content). This includes Emails that do not reach their destination such as spam, malware infected or quarantined.
  - Logging of all websites visited.
  - Logging of all communication blocked by our security products e.g. Anti-Virus or Firewall threat prevention.

- Auditing:
  - Auditing records are kept on some systems and databases which can give forensic analysis of activities and transactions that have taken place.

- Data loss Prevention:
  - A minimum level of automatic Data Loss Prevention(DLP) techniques are in operation on both the Email communication and Web traffic. This may quarantine or prevent the information from being sent or received.

PMC6 – Recording Relating to Network Connections

Control Description:

- To monitor transient connections to the network such has remote access, virtual private networking, wireless or any other temporary connection.

Aberdeen City Council Control Process in Place:

- Authentication:
  - Necessary for all network access is authentication. Authentication is required whether you are on the main network, wireless network, connecting remotely, over a Virtual Private Network (VPN) or are a 3rd party.

- Logging:
  - Such connections will be logged by various systems such as the Firewall, Directory Services and DHCP. Information that is logged varies but may include, source IP Address, source device, destination IP address, destination device, Logon date/time, Logoff date/time, Username.

PMC7 – Recording of Session Activity by User and Workstation

Control Description:

- To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.

Aberdeen City Council Control Process in Place:

- Logging:
    - System logs indicating both successful and unsuccessful logins are recorded within some systems.
    - Logging of all Emails sent or received takes place (not the content). This includes Emails that do not reach their destination such as spam, malware infected or quarantined.
    - Logging of websites visited by users.
    - Logging of all communication blocked by our security products e.g. Anti-Virus or Firewall threat prevention.
- Auditing
    - Auditing records are kept on some systems and databases which can give forensic analysis of activities and transactions that have taken place.

PMC8 – Recording of Data Backup Status

Control Description:

- To provide a means by which previous known working states of information assets can be identified and recovered from in the event that either their integrity or available is compromised.

Aberdeen City Council Control Process in Place:

- Backups of system shares and drives are performed to a schedule. Tests are regularly performed to ensure integrity and recovery.

PMC9 – Alerting Critical Events

Control Description:

- To allow critical events to be notified in real-time.

Aberdeen City Council Control Process in Place:

- Alerts can be automatically generated when:
    - There are unexpected deviations from normal traffic levels.
    - The status or performance of infrastructure equipment across the organisation changes.
    - There are unexpected deviations from normal monitoring or the status of Firewalls changes.
    - There are attempted failed changes to elevate privileges on domain servers.