Digital Security – Monitoring and Standards

Contents:

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Digital Security

Background

Protecting the council's digital information assets is key to delivering the council's digital strategy. A failure of confidentiality, integrity or availability could have a significant effect on the ability of the council to deliver its services via digital platforms. This policy sets out the minimum requirements for access to the council's digital resources.

Key Messages

The latest version of the software/firmware will be installed as soon as practicable.

The data environment will be monitored and reported upon.

Devices in use by our organisation will adhere to configuration standards.

Where the principles in this policy cannot be met, the risk must be recorded in the ICT Risk Management and Accreditation Database (RMAD) and authorised by the appropriate SIRO.

Policy Detail

Protective Monitoring

Protective Monitoring is a set of processes utilising technology or manual process that need to be in place in order to oversee how ICT systems are used; assuring user accountability for the use of ICT facilities.

The goal of protective monitoring is to provide assurance that the confidentiality, integrity and availability of the council's digital resources are maintained and to meet the requirement of any compliance sets and legal obligations that pertain to these resources (eg PSN, PCI-DSS, DPA, Computer Misuse Act)

It is not practical to set out every item of protective monitoring in this section of the policy. EKS ICT will maintain operational procedures to achieve the following (as a minimum) and consider the event conditions and uses cases as set out in Appendix 3.

- Who, What, How and When the network was accessed.
- Password abuses.

- Email and Web traffic.
- Malware detection.
- Software, Firmware and Operating system patch levels
- Intrusion detection
- Data Leak detection

Protective Monitoring logs may be provided to external agencies.

Protective Monitoring logs must be maintained for 12 months.

Protective Monitoring logs must be protected against unauthorised changes.

PCI-DSS SAQ D - Requirement 10 (Track and monitor all access to network resources and cardholder data) will be considered

Software Standards and Patch Management.

This section of policy sets out the standards and requirements that will be adhered to in the operation of the council's Software and Infrastructure assets.

Every council owned and managed device that can receive a firmware update and/or software update that accesses the council's Digital resources is in scope.

Key Messages

- The latest version of the software/firmware will be installed as soon as practicable.
- Un-patchable software will not be used.
- The software environment will be monitored and reported upon.
- Where these principles cannot be met, the exemption must be recorded in the ICT RMADS and authorised.

Patch management refers to the process by which an organization installs patches, which are fixes or updates to computer programs, operating systems, or applications. Patch management is an important element in mitigating the significant security risks associated with software vulnerabilities.

From an operational perspective, updates fix known flaws and bugs and sometimes provide new functionality. When a software vulnerability is discovered, the software vendor may develop and distribute a security patch or work-around to mitigate the vulnerability. Any significant delays in finding or fixing software with critical vulnerabilities provides opportunity for persistent attackers to break through, gain control over the vulnerable machines, gain access to the sensitive data contained on the computer, destroy information on the computer, or use the computer as a launching point for additional attacks to other computers on the network.

Outdated and unsupported software is more vulnerable to attack and exploitation. The majority of vulnerabilities exploited by viruses are ones for which a fix is available from the software vendor.

The councils are responsible for the security and integrity of the network, servers and IT Infrastructure. As part of the overall approach to maintaining the security, confidentiality and integrity of the network, this policy sets out the standards, responsibilities and approach that the IT provider will adhere to in the maintenance of the software and firmware environment.

This policy applies to all hosts that are connected to the corporate network. This includes, but is not limited to, Servers, Workstations, Network Infrastructure, SANs, Firewalls. It is the responsibility of everyone to work together to ensure that systems and devices they operate and use are maintained in accordance with this policy.

The risks and difficulty associated with updating firmware warrant a different standard to that of Operating systems and Application standards. A failure during the updating of firmware can lead to catastrophic, permanent failure of that equipment. For these reasons, it is not required that Firmware is updated upon release of new firmware by the manufacturer. Firmware must be updated to the latest stable release during commissioning of that infrastructure. Thereafter, it is required that firmware is updated if a security vulnerability (CVSS 4.0 or greater) is discovered within a release or to add desired functionality.

Hosts or applications found to be in breach of this policy may be disconnected from the network or have measures applied that reduce the risk, for example disabling internet access or limiting onward access. These measures may restrict non business critical functionality (eg disabling internet access from the affected system).

The network will be scanned quarterly for vulnerabilities and those vulnerabilities reported to the relevant technical manager, information asset owner and organisation PCI DSS risk officer.

Critical vulnerabilities must be resolved within 14 days, important vulnerabilities within 30 days and all others within 60 days.

Where it is known that a vulnerability is being actively exploited then mitigating action (e.g. patch applied) should be taken immediately.

Where a patch or mitigation is not deployed (or available) within the timescales above then there must be alternative mitigating action, such as disabling or reducing access to the vulnerable service.

Device Management Standards.

The councils will ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability. In particular applications, services, processes and ports not required are disabled by default. Default passwords will be

changed. Configuration control of applications installed and administrative oversight of devices will be maintained.

Users are only allowed minimum desktop customization, and are not permitted to make changes to system configuration settings (such as Antivirus, network settings or Update management) or have rights to install extra software (Local Admin).

All changes will be recorded, managed and authorised.

All owned and managed devices must meet these criteria.

- The device should be encrypted to protect data at rest
- The boot process should be secured so that it cannot be modified by unauthorised software or personnel
- All capable devices must have the capability to detect, isolate and respond to malicious software.
- The device must have the capability to report security events to the appropriate enterprise audit and monitoring services. The user must be prevented from tampering with the reporting of events.
- The device is able to constrain the set of ports (physical and logical) and services exposed to untrusted networks and devices.
- The device must be capable of receiving policy based configuration from the management platform (e.g. Active Directory/MDM)

Note: If suppliers request details of our standards, please refer them to this Government document and ask them to provide written assurance that they operate systems that meet these principles.

https://www.gov.uk/government/publications/end-user-devices-security-principles/end-user-devices-security-principles

Variation from Policy

The councils accept that occasionally, for operational reasons, it is not always possible to adhere closely to this policy. Requests for exemption will be considered by affected SIROs and granted on the merits of an individual case. Exemptions (and associated mitigations) will be recorded in the ICT Risk Management and Accreditation Database (RMADS) and reviewed by the CIGG.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Incident Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
03/08/2016	Will Causton	1.0	Initial Version
23/09/2016	Will Causton/CIGG	1.1	Amended following CIGG Consultation
05/10/2016	Hannah Lynch	1.2	Final Formatting

Appendix 1: Protective Monitoring Controls

The Public Sector Network Code of Connection states:

"You will collect and retain event data and undertake activities that will help you detect actual or potential security incidents. You must have a protective monitoring policy that describes the use cases you are aiming to detect, which can be used to define event data collection.

Your policy must include both detection of technical attacks as well as important abuses of business processes. These conditions do not describe any specific events to collect or incidents to detect. The requirement is that the business has thought about and documented its collection and analysis requirements and that this has led to your approach to protective monitoring and intrusion detection."

The councils want to identify:

- Who? What? How? and When the network was accessed.
- Abuses of the Password policy.
- Abuses of Email and Web traffic.
- Malware Activity
- Software, Firmware and Operating system patch levels
- Intrusion detection
- Data Leak detection
- The use of unauthorised devices to access the council's Digital resources.

To achieve these aims, combinations of the following protective monitoring controls will be used.

Accurate Time in Logs

All devices shall use a common time source so that logs may be correlated. Internal time servers will use ntp.gcsx.gov.uk as their source.

Traffic Crossing a Boundary

Boundary firewalls will report connection details to the Syslog service.

Suspicious Activity at the Boundary

IDS and IPS will be operated at the boundary, logs will maintained within the IDS/IPS system. Critical events will be alerted in real time to the NOC Console.

Internal Workstation, Server or Device Status

Logs will be maintained of when hosts connected and for how long they were connected.

Logs will be maintained of USB devices connected or disconnected to a device.

Suspicious Internal Activity

User logon records will be reviewed for suspicious behaviour.

Password logs will be reviewed and challenged daily.

Changes to privileged active directory groups alerted in real time to the NOC Console

Network Connections

Network infrastructure will report 802.1x events to the syslog service; unknown devices will be alerted in real time to the NOC Console.

Session Activity by User and Workstation

Logon/logoff for machine and user accounts will be recorded in multiple locations, including, Active Directory Event log and AD Audit+ SIEM system.

Backup Status

The status of backup events will be alerted to the backup console and reviewed daily.

Email and Web traffic.

Web traffic from the corporate network will be logged.

Metadata (Sender, Recipient, Date, Time, Subject line and file name of any attachment) will be logged.

Management reports produced monthly

Malware detection and Data Leak detection

All malware and data leak events will be logged.

The Malware Detection console will be checked daily that the estate is able to update.

Malware detection events will be reported in real time to the service desk console.

Data leak detection events will be reported in real time to the NOC Console

The data leak prevention feature will alert on the following information patterns

- National Insurance Numbers
- Credit or Debit Card numbers.
- Bank account numbers
- The word “password”

Software, Firmware and Operating system patch levels.

A vulnerability scanning tool (Nessus) will be used to conduct a credentialed vulnerability scan quarterly.

Solar Winds Patch Manager (for Third party applications) and Microsoft Windows Update services will maintain logs of updates that have been installed and used to produce management reports about the status of patch levels.

Smart Devices

The configuration and location of Smart Devices will be monitored by the MDM platform.