ICT Virus and Malware Protection Policy

Document version	1.0
Drafted by	ETBI ICT Group
Responsibility for this policy in City of Dublin ETB	Director OSD/Head of ICT
Reviewed by Senior Leadership Team (SLT)	24/09/2024
Approved by Chief Executive	24/09/2024
Noted by Board	17/10/2024
To be reviewed	1 year from CE Approval

Contents

1 Introduction

1.1 Purpose of this Document

The Virus and Malware protection policy is defined in the City of Dublin ETB ICT Framework Policy and should be read in conjunction with all other ICT policies to ensure required security standards are adhered to. The purpose of this Virus & Malware protection policy is to define a standard to prevent, detect and remediate virus and malware infection in City of Dublin ETB environment.

1.2 Scope and Constraints

The scope of this policy applies to all Users within City of Dublin ETB**.**

1.3 Definitions

A full range of definitions is available in the ICT Frameworks Policy.

1.4 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, who are committed to continually improving the protection of all City of Dublin ETB information assets and the protection of personal data where City of Dublin ETB is a controller or processor. This document will be reviewed at least annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within the City of Dublin ETB

2 Policy / ICT responsibilities

For the purpose of this policy, the term "virus" is generically applied to all malicious software that performs malicious tasks such as deleting files, changing computer settings, or collecting personal information. This includes Viruses, Worms, Malware, Trojans, Spyware, Adware, Rootkit, Bots, *etc*.

City of Dublin ETB employs an 'in-depth defence' strategy to minimise the risk of loss or damage to services as a result of a virus outbreak. This includes a layered security approach at:

a) Network Perimeter
b) Server Level
c) Client (Local) Protection
d) Mobile Devices

The following applies to all layers listed above:

- Standards and guidelines should be published which specify: methods for installing and configuring anti-virus, provisioning of updates, processes required to review the effectiveness of the anti-virus protection.

- Anti-virus used must be configured to protect against all forms of Viruses, Worms, Malware, Trojans, Spyware, Adware, Rootkit, Bots, *etc*.

- Anti-virus must be distributed and updated automatically with defined timescales to reduce the likelihood of attacks.

- Anti-virus must be configured to scan firmware, master boot record (MBR), targeted files such as executables, and protected files.

- All desktop PCs, laptops, and servers must be scanned by anti-virus at least once a week.

- In the case where anti-virus must be modified or disabled, this should be formally approved based on a specific business requirement and by the ICT Dept, Asset owner. The period of disablement or change must be restricted to a minimum.

- All systems and devices must be monitored to detect inactive, misconfigured, and out of date anti-virus
  a) If disabled anti-virus is detected, this must be automatically re-enabled as soon as possible. Unless formally approved.
  b) Any outdated anti-virus must be updated in a timely manner as per a pre-defined timeline (such as 14 calendar days)
  c) Where possible, if a device's anti-virus has not been updated in a pre-defined timeline (such as 14 calendar days), it must be blocked from connecting to the corporate network until the updates have occurred.

- A process for responding to and remediating virus incidents/infections must be defined and implemented.

2.1 Anti-Virus at the Network Perimeter

- Perimeter protection software ("security proxy") must be provided for each security domain crossing point meeting one of the following properties:

  a) One of the domains in question is exposed/susceptible to attack, or

  b) One of the domains in question is considered less secure than the other domain, in terms of protection against malware.

  This is especially the case if one of the domains is the Internet, but is also valid if one of the domains belongs to a different operating company and/or vendor.

- Anti-virus checks must be enabled on Web Proxies to the Internet.

- All network traffic entering and leaving the corporate network, including email, must be scanned and protected by anti-virus.

- Test and non-production systems which are connected to a corporate network, or can be accessed from a system on the corporate network, must be protected by anti-virus.

2.2 Anti-Virus Server Protection

- All Microsoft-based Servers must have anti-virus software installed and active. This includes:

  a) Real-time “on-access” scanning.

  b) Weekly scan for malicious code.

- All anti-virus software must be configured to be updated automatically using a centralised update system with the ability to push updates to the anti-virus client as required. The Virus Signatures should be updated (at a minimum):

  a) Daily for servers with network access to virus signature update server

  b) Weekly for other non-network connected servers

- UNIX-based servers currently do not need virus protection software for system areas (due to the fundamentally different approach for UNIX file system security, User permissions, and executables not depending upon extension). However, UNIX-based systems are not bulletproof and can still suffer from malware and Trojans. For critical systems or systems that perform a high level of interactivity with users, a risk assessment must identify if Virus protection is required on UNIX-based systems.

  a) Where anti-virus cannot be deployed on Linux and Unix-based systems, protection must be provided through implementing security hardening, host-based firewalls, with critical assets being protected by network-based controls.

- For highly sensitive and critical systems, file system integrity tools (*e.g.* "tripwire") should be implemented and configured to check the integrity of the system environment daily. Such tools follow the principle of setting up an initial list of cryptographic checksums (covering each file in the system environment) followed by periodic checks (comparison of newly calculated checksums against the initial list).

- Servers with other operating systems than MS-Windows or UNIX are currently out of scope (*e.g.* Tru64/OpenVMS etc). In case such systems must be used, a case-based consultancy and evaluation must be carried out by the operational security staff.

- Endpoint detection and response (EDR) should be enabled on all supporting servers. EDR rule content must be continually reviewed and updated, in line with the latest available threat intelligence.
- Where an exception is requested not to install anti-virus (*e.g.* product does not support anti-virus), compensating controls are required to limit the exposure to viruses and malware. If an exception is permitted it must be recorded on the local risk register and assigned to the Asset Owner. This may be in the form of whitelisting of allowed processes.

2.3 Anti-Virus Client (Local) Protection

Client protection is the third level of protection against viruses and malware. Since there are ways to bypass the security proxies or servers (*e.g.* loading data from portable storage media like CD or USB sticks), this level of protection is at least as important as perimeter protection.

- All desktop and laptop IT equipment must have anti-virus software installed and active and must comply with the following requirements:
  a) Installation must be enforced by a centralized network installation tool prohibiting any user interference.
  b) Automated updates of Virus Signatures must be performed a minimum of once a day with integrity and authenticity checking based on signatures and/or cryptographic hash values or comparable secure mechanisms must be available.
  c) Behavioral-based AV detection must be in use.
  d) Provision of log data generation and central storing must be provided.
  e) Online (real-time) scanning must be enforceable as a background service (each file access must be checked).
  f) Online (real-time) scanning must include all available storage resources files could be loaded from (e.g. network shares);

  Attention: this requirement explicitly includes MBRs (of a whole medium as well as of a partition)
  g) Online (real-time) scanning configuration must not be modifiable with user privileges.
  h) The possibility of manual runs (explicit file checking) must be provided.
  i) Configurable actions on malware must be provided; at least deletion of malware and information of the involved user must be selectable.
  j) Automated scanning of portable storage media should be conducted whenever accessed or executed.

- Whilst checking local file access, the local scanner should be able to generate at least the following information on files containing malware or suspicious content:
  a) **[host IP address**
  b) **hostname (DNS name)**
  c) **VLAN access for the infected device**
  d) **filename (full path name including hostname)**
  e) **file type**
  f) **timestamp**
  g) **pattern ID/malware description**
  h) **executed action]**

- Endpoint detection and response (EDR) should be enabled on all supporting clients. EDR rule content must be continually reviewed and updated, in line with the latest available threat intelligence.

2.4 Anti-Virus Mobile devices Protection

Anti-virus must be incorporated on all mobile devices owned by City of Dublin ETB or where confidential information regarding City of Dublin ETB can be accessed. This includes network infrastructure.

- All mobile devices must be up to date and gain continuous updates from their respective manufacturers.

- All mobile devices must be enrolled in City of Dublin ETB mobile device management.

3 User Responsibilities

- Users must not attempt to disable antivirus.
- Users must not interfere with the scheduled scan process.
- Users must not install un-approved antivirus software.

4 Enforcement

Individuals found to be in breach of this policy, may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

5 References

ISO27001	NIST CSF	PCI-DSS