# ICT Firewall 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 | 22/10/2024 |
| To be reviewed | 1 year from date of approval by CE |

# Contents

# 1. Introduction

## 1.1 Purpose of this Document

The Firewall Policy is defined in City of Dublin ETB's ICT Framework Policy and should be read in conjunction with all other ICT policies to ensure that required security standards are adhered to. This policy document defines the ICT Department standards regarding the management and maintenance of firewalls at City of Dublin ETB and it applies to all firewalls owned, rented, leased, or otherwise controlled by City of Dublin ETB.

## 1.2 Scope and Constraints

The scope of this policy applies to all firewalls on all City of Dublin ETB networks, whether managed by direct employees or by third parties. In some instances, systems such as routers, air gaps, telecommunications front ends, or gateways may be functioning as though they are firewalls when they are not formally known as firewalls. All City of Dublin ETB systems playing the role of firewalls, whether they are formally called firewalls, must be managed according to standards defined in this policy. In some instances, this will require that these systems be upgraded so that they support the minimum functionality defined in this policy, these upgrades may need to be completed as part of a phased project plan.

## 1.3 Definitions

A full range of definitions is available in the ICT Framework 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 every year by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within the organisation.

# 2. Firewall Configuration / ICT responsibilities

- Only authorised and qualified personnel, such as firewall administrators, may access and make changes to the firewall devices.
- All firewall rules must be fully documented and recorded to include the following:
  - Change management procedures (when making configuration changes to firewall rules or firewall devices),
  - Rollback procedures (for when a change does not have the desired effect).
- All configuration changes must be fully tested in a non-production environment for verification prior to implementation on live systems.

- Firewall rules which allow temporary access should have a specified lifetime and access must be revoked at the termination of the specified period.

- The business requirements for rule changes to firewall must be approved by the Head of IT and documented for verification prior to implementation on live systems.

- Network architecture diagrams should accompany the strategic deployment of both perimeter and internal firewalls.

- Decommissioning of firewall devices must be conducted in compliance with the organisational ICT asset management policy.

- All default access credentials must be removed from firewall devices prior to deployment to live environments.

- All firewalls must have a unique password with Multi-factor Authentication (MFA) or other access control mechanisms. Where management interfaces are used, they should be locked down to specific hosts and only secure management protocols used. The same password or access control code must not be used on more than one firewall.

- Where the firewalls are cloud managed, the vendor cloud management account should have MFA enabled.

- All firewall rules should be intuitively named to reflect the purpose of each rule.

- Firewall rule configurations must be reviewed at regular intervals and all redundant rules must be removed.

- For firewalls managed directly by City of Dublin ETB, backups of up-to-date running configurations for all firewalls must be available and must be tested regularly, and conducted in compliance with the [ICT Backup and Restore Policy. Where possible, an automated backup procedure should be put in place.

- Security patches and firmware updates should be applied in compliance with and in line with vendor recommendations.

- Administration accounts should be uniquely identifiable, *i.e.* they should not be generic.

- Firewall activity logs must be monitored and regularly reviewed for unusual activity using a SOC/SEIM service

- Where possible logs should be stored externally (*e.g.,* Syslog server) and a mechanism implemented to alert administrators of critical events on the firewall

- Only OGP approved firewalls may be deployed within the City of Dublin ETB network.

- Firewalls must be placed in a restricted access area, with air-conditioning and an uninterruptible power supply.

- Physical access to the Firewall rooms must be logged and monitored. It must also be equipped with alarms.
- SSL Certificate inspection and virus scanning must be enabled on all capable firewalls.
- All Servers that are exposed to the internet must be placed in the Demilitarized Zone (DMZ).
- Firewalls must be considered within the business continuity plans for the organisation, any secondary/failover configuration must be fully documented and tested.
- A management report which contains all open firewall ports along with justifications and ownership is to be documented and signed off annually

## 3. User responsibilities

- No unauthorised user is permitted access to any City of Dublin ETB Firewall device.
- Any suspicious activity should be reported to the Head of IT
- Users must not attempt to circumvent City of Dublin ETB software or hardware firewall rules of any kind.

## 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 |
|---|---|---|
| | | |

# 6. Appendix A

A management chart of firewall rules such as the below should be maintained for review purposes

| Rule Name | Port open | Source address | Destination address | In bound / out bound | Business Requirement | Owner / Approver | Review Date |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |