FIREWALL POLICY

Policy Code: TM3
Version: 3
Approved by: The Board
Approval Date: 11/04/2024
Decision No.: B01.2024.03

Table of Contents

1 INTRODUCTION 3
2 DEFINITIONS 4
3 REGULATORY FRAMEWORK 5
4 SCOPE 6
5 PURPOSE 6
6 RESPONSIBILITIES 6
7 CHOICE OF FIREWALL TECHNOLOGY 6
8 FIREWALL DESIGN IMPLEMENTATION 7
9 FIREWALL MONITORING 7
10 FIREWALL BACKUP 7
11 INTRUSION DETECTION 8
12 OPERATING SYSTEM HARDENING 8
13 REMOTE MANAGEMENT 8
14 TIME SYNCHRONISATION 8
15 ANTI-VIRUS 8
16 CHANGE RULESET REQUESTS 8
17 BREACH AND ENFORCEMENT 9
18 THIRD PARTY\FOREIGN DEVICE\USER CONTROL 9
19 REVIEW OF POLICY 9
20 REVISION HISTORY 10

1 INTRODUCTION

The Da Vinci Institute is a registered private higher distance education provider (Registration No. 2004/HE07/003) offering accredited qualifications on NQF levels five to ten, which are registered on the Higher Education Qualifications Sub-Framework (HEQSF). This policy forms part of the institutional Integrated Quality Management System and details the principles for ensuring that programme offerings adhere to the required academic regulatory standards and empower students to contribute to the transformation of their communities, society, and the economy of the future. This approach is underpinned by the Business- and Community-based Action Learning discourse on the co-creation and distribution of relevant knowledge.

The Institute has perimeter firewalls between the Internet and its network in order to create a secure operating environment for its equipment connected to its network.

The firewall is an appliance (a combination of hardware and software), or an application (software) designed to control the flow of Internet Protocol (IP) traffic to, or from a network or electronic equipment. Firewalls are just one element of the layered approach to network security and are used to examine network traffic and enforce policies based on instructions contained within the firewall's ruleset. Firewalls at The Institute's represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to antivirus software, intrusion-detection software, strong passwords/passphrases, and spyware detection utilities.

The Firewalls are categorised as either 'Network' or 'Host' and are appliances attached to the network for the purpose of controlling access to single or multiple hosts, or subnets. The host firewall is an application that addresses an individual host (e.g., a personal computer) separately. Both types of firewalls (network and host) could be used jointly.

The role of the firewall is to protect The Institute's equipment and restrict unwanted access to the network. The firewall will (at minimum) perform the following security services:

a) Access control between The Institute's network and untrusted external networks
b) Block unwanted traffic as determined by the Firewall ruleset.
c) Hide vulnerable internal systems from the Internet.

d) Hide information, such as system names, network topologies, and internal user IDs from the internet.
e) Log traffic to and from The Institute's network.
f) Provide robust authentication.

2 DEFINITIONS

Term	Definition
Access Control	The rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of information security is based upon access control, without which information security cannot, by definition, exist.
Computer Network	A set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the internet. Other shared resources can include a printer or a file server.
Equipment	Include computers, desktops, servers, network devices/printers, laptops, telephones, cell phones, electronic handheld devices, tablets/mobile devices, facsimile machines, software, hardware and/or similar equipment owned by, licensed to, or rented by The Institute, or user equipment that are utilised during business hours at The Institute.
Firewall	Includes hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorised access while permitting authorised communications to or from a network or electronic equipment.
Firewall Configuration	The system settings affecting the operation of a firewall appliance.
Firewall Ruleset	A set of policy statements or instructions used by a firewall.
Foreign Device	Any electronic device that requests access to the Da Vinci Network or Platform but does not belong to Da Vinci Institute.
Hardening	In computing, hardening is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one. Reducing available ways of attack, typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.
Host	Any computer connected to a network.
Legally/Contractually Restricted Information	Information that is required to be protected by an applicable law or statute (e.g. Protection of Personal Information Act 4 of 2013 (POPI) which, if disclosed to the public, could expose The Institute to legal or financial obligations. Examples include, but

Term	Definition
	are not limited to occurrences of personally identifiable information, such as, personnel records, student records, names in connection with ID numbers, and credit card numbers.
Network	The network infrastructure and associated devices including but not limited to network devices provided or served by The Institute.
Network Devices	Any physical equipment attached to The Institute's network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to, routers, switches, hubs and wireless access points.
Network Firewall	A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).
Sensitive information	Is data that must be protected from unauthorised access to safeguard the privacy or security of an individual or organisation.
Third Party/Foreign user	A third party/Foreign user is defined as any individual, consultant, contractor, vendor, student, alumni, faculty member, or agent who is not employed by the Da Vinci Institute.

3 REGULATORY FRAMEWORK

This policy is benchmarked against and should be read in the context of the relevant legislation underpinning the principles against which institutional policies and operational procedures are developed, implemented and maintained. These include:

A. Relevant legislation:
   i. Constitution of the Republic of South Africa (No.108 of 1996)
   ii. Electronic Communications and Transactions Act (No. 25 of 2002)
   iii. Films and Publications Act (No. 65 of 1996)
   iv. Promotion of Access to Information Act (No.2 of 2000)
   v. Protection of Personal Information Act (No.4 of 2013)

B. Applicable Da Vinci documents:
   i. A4 – Privacy and Confidentiality Policy
   ii. A12 – Records Management Policy
   iii. B25 – Social Media Policy
   iv. C1 – Electronic Information and Communication Systems
   v. C2 - Acceptable Use of Information Technology Systems Policy
   vi. C3 - Information Security Management Policy
   vii. C5 - Wireless Communication Policy
   viii. C7 – Incident and Service Management Policy

ix. C8 - Disaster Recovery Information Technology Policy
x. Third Party/Foreign user Network Access Agreement Form

4 SCOPE

This policy applies to all The Institute's employees and other persons who have access to, and use The Institute's equipment to create, access or use The Institute's information systems connected to The Institute's network.

5 PURPOSE

The purpose of this policy is to:

a) Describe how the firewall will filter internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for business users.
b) Provide criteria on when firewalls are required or recommended. A network firewall is required in all instances where sensitive data is stored or processed. A host firewall is required in all instances where sensitive data is stored or processed and the operating environment supports the implementation. Both the network and host firewalls afford protection to the same operating environment, and the termination of controls (two separate and distinct firewalls) provide additional security in the event of a compromise or failure.
c) Raise awareness on the importance of a properly configured (installed and maintained) firewall.

6 RESPONSIBILITIES

The Institute's Information and Communication Technology (ICT) department is responsible for implementing and maintaining firewalls.

Logon access to the firewall will be restricted to a primary firewall administrator and one designee. Password construction for the firewall will be consistent with strong password creation practices.

Any questions or concerns regarding The Institute's firewall should be directed to the Head of Information and Communication Technology.

7 CHOICE OF FIREWALL TECHNOLOGY

Firewalls are chosen based upon their history of security and particular features fit to the desired task. Firewall solutions deployed are configured to support the minimum required options for firewall technology. All new technology shall be configured by the IT Department in accordance with this policy.

8 FIREWALL DESIGN IMPLEMENTATION

a) The firewall design allows minimum access required through the firewall for business purposes.
b) Consideration is made according to:
    I. Risk and Threat Assessment
    II. Administration
    III. Monitoring
    IV. Configuration Management
    V. Intrusion Detection System.
c) Firewall rulesets are based upon a default deny principle and rule. The Institute's firewall permits the following outbound and inbound internet traffic:
    I. Outbound – All Internet traffic to hosts and services outside of The Institute
    II. Inbound – Only Internet traffic from outside that supports the business mission of The Institute.
d) Firewalls must be installed within production environments where Legally/Contractually Restricted Information is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.
e) IT will maintain a database of the most common services that will be accepted or denied. This data will be maintained in accordance with the needs of the business and will be available on request from the Head of Communication and Information Technology.

9 FIREWALL MONITORING

Firewall monitoring include the following actions:
a) Monitor firewall logs
b) Monitor network traffic
c) Store logs related to firewall ruleset changes and attack attempts, in a separate location for internal audit and archiving purposes.

10 FIREWALL BACKUP

a) Firewall rulesets and configurations must be backed-up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required.
b) Access to rulesets and configurations and back-up media must be restricted to those responsible for administration and review.

11 INTRUSION DETECTION

Appropriate technology is used to detect intrusion attempts.

12 OPERATING SYSTEM HARDENING

Firewalls installed onto base operating system-build are hardened before being deployed. Hardening is in accordance with The Institute's requirements and standards.

13 REMOTE MANAGEMENT

a) Remote management of the firewall is done through Secure Shell (SSH) or HyperText Transfer Protocol (HTTPS) where the protocol is mapped to an alternate port.
b) Remote access to the firewall should be restricted through an Access Control List (ACL) as and when required.

14 TIME SYNCHRONISATION

All firewalls must have time synchronised via Network Time Protocol (NTP) from multiple approved internal time sources.

15 ANTI-VIRUS

Anti-Virus controls will be implemented in accordance with The Institute's *C3 - Information Security Policy*. Controls must be implemented where data is capable of containing viruses or where possibility exists for malicious code traversing through the firewall.

16 CHANGE RULESET REQUESTS

a) The Institute's employees may request access to previously disallowed traffic, which will result in the firewall's configuration change, subject to:

    I. A firewall Change Request form, with full justification, must be submitted to the IT department for approval;
    II. All requests will be assessed to determine if they fall within the parameters of acceptable risk;
    III. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original person requesting the access, and alternative solutions will be explored;

IV. Turnaround time for the above stated firewall reconfiguration and network access requests is approximately six (6) days from the receipt of the request form.

b) The Institute's employees may request access from the Internet for services located on The Institute's network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection. VPN sessions will have an absolute timeout length of one (1) day. An inactivity timeout will be set for one (1) day. At the end of these time-out periods, users must re-authenticate to continue or re-establish their VPN connection. A VPN Connectivity Request form, with full justification, must be submitted to the IT department for approval. Approval is not guaranteed that the request for access will be granted.

c) From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to The Institute's internal network. If such a need arises, a Third-party Access Request form, with full justification, must be submitted to the IT department for approval. Approval is not guaranteed that the request will be granted.

17 BREACH AND ENFORCEMENT

Wherever possible, technological tools will be used to enforce the requirements of this policy and mitigate security risks. Any failure and/or refusal to comply with the provisions of this policy may result in disciplinary action which may include dismissal or liability for damages.

18 THIRD PARTY\FOREIGN DEVICE\USER CONTROL

The Third party may only use the network connection for approved business purposes as outlined in the Third Party/Foreign user Network Access Agreement Form
to be completed online - https://forms.office.com/r/3CttDgWJjS

19 REVIEW OF POLICY

Regular review and amendments of this policy will be done in line with the approved institutional policies. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodians of this policy, namely the Head of Information and Communication Technology.

20 REVISION HISTORY

Version No.	Amendment Details	Approval date	Approving Committee	Chairperson Signature
Version 1 (V1)	Various	25/02/2022	EXCO	
Version 2 (V2)	Amendments as per review tracking document: Amendment review	11/04/2024	The Board	B.01.2024.03