This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Proxy Security Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements related to proxy solutions in <organization name>.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to(ECC-1:2018), in addition to other related cybersecurity legal and regulatory requirements.

Scope

The standard covers <organization name>'s information and technology assets and applies to all personnel (employees and contractors) in <organization name> and related third parties.

Standards

1	General Requirements
Objective	The proxy solution must be securely configured, managed and appropriately used when required to prevent entering a private network.
Risk Implication	Misconfiguration of proxy solution may create vulnerabilities that may lead to information theft, unauthorized access and information disclosure.
Requirements	
1-1	All the following requirements are relevant for and must be applied for all types of proxy solutions included in Table A.
1-2	Physical access to the proxy server must be monitored and restricted only to authorized employees (least privilege assignment for different administrators).

1-3	Unused Network Information Collectors (NICs) must be disconnected from any network.
1-4	Proxy server must support IPv4 and IPv6 stack for traffic processing and security rules, traffic policy definition.
1-5	All security updates to the proxy server must be installed, as they are released by the vendor according to <organization name>'s change management procedure.
1-6	Ensure that proxy server can be deployed in various methodologies - inline, transparent proxy, explicit proxy, span - described in Table A, according to <organization name>'s network architecture.
1-7	All management communication channels must be using a dedicated management network, or the management network communications is authenticated and encrypted using cryptographic modules compliant with National Cryptography Standard.
1-8	Administrative access to the management interface of the proxy server must be restricted to authorized administrators only.
1-9	Time configuration on the proxy server must be synchronized with a trusted authoritative time server.
2	Traffic shaping
Objective	Proxy server must be properly configured and securely managed in order to properly filter network connections.
Risk Implication	Misconfiguration of traffic shaping rules may have severe consequences like legitimate traffic blocking and denial of service.
Requirements	

2-1	Proxy server must provide a traffic control policy which allows to specify least source and destination IP address, TCP port, logging options.
2-2	Administrative users must have the possibility to configure static lists of always available or denied resources that must be verified by proxy server during traffic processing.
2-3	Proxy server must recognize, Uniform resource identifiers, URLs, applications (based on signatures), IP addresses, TCP ports.
2-4	Proxy server must have the ability of caching the most frequently used web objects to optimize traffic bandwidth and delay.
2-5	Proxy server must have the ability to suppress, add, or rewrite packet headers.
2-6	Proxy server must provide the ability to verify compliance to protocol standards and prevent traffic that is not compliant (or correcting and fixing non-compliant traffic). For example, the streaming proxy can completely stop a buffer overflow attack, using protocol compliance enforcement.
2-7	Proxy server must provide the ability to translate protocols from one side of the conversation to the other. For example, if a client is only capable of IPv4, the proxy can be used to proxy a conversation to an IPv6 web server, enabling access even without IPv6 support on the client side. Likewise, an IPv6-only client or environment can access an IPv4 web server through a web proxy.
3	Traffic inspection
Objective	Proxy servers must process traffic in a secure way to careful evaluate and check for signs of abnormal or malicious behavior.

Risk Implication	Traffic processing without a security layer may easily cause malware propagation, phishing exposure and information leak.
Requirements	
3-1	Proxy server must deliver a built-in URL categorization base, divided into various categories, like phishing, news, drugs, medical, banking, etc.
3-2	Proxy server must have an antivirus engine to filter all objects transferred to clients and EDR to identify suspicious behavior. Antivirus engine must be consistent with the requirements of <organization name>'s Malware Protection Standard.
3-3	Proxy server must have a built-in application base divided into various categories, like VPN, dating, tor-proxy, etc.
3-4	URL categorization base, application and virus signatures must be updated at least daily.
3-5	Proxy server must analyze the whole communication, including packet headers, parameters of HTTP request, web objects, scripts, etc.
3-6	Proxy server must have a possibility to intercept the SSL/TLS-secured traffic - decrypt, inspect and encrypt specified communications.
3-7	During the SSL-inspection process, the proxy server must use a certificate signed by <organization name>'s certificate authority.
3-8	Administrative users must have a possibility to exclude some communication from inspection (for example SSL intersection process).
3-9	Administrative users must have a possibility to integrate proxy server with other security solutions like sandboxing, CASB, DLP etc. using industry-standard interfaces such as ICAP.

3-10	Proxy server must prevent access to the web resources by unauthorized users by captive portal enforcement or by integration with the <organization name>'s authorization system.
3-11	Proxy server must inform user about performed actions (in particular: blocked requests or files) by configurable response web pages.
3-12	Proxy server must use security feeds delivered by national trusted organizations like national level CSIRT.
4	Logging and Monitoring
Objective	All sensitive events related to proxy security must be monitored and stored for the proactive detection of cybersecurity attacks.
Risk Implication	Without proper configuration of logging, it is not possible to investigate performance, network attacks and control cybersecurity measures like KPI, compliance and governance violations.
Requirements	
4-1	Proxy server must be configured to log events and audit logs to the central log system.
4-2	Proxy server must gather events in separate files especially for audit and traffic events.
4-3	Proxy server must log all URL requests, denied sessions and threat events.
4-4	Proxy server must gather in audit log file at least events related to failed and successful login to administration interfaces.
4-5	Proxy logs must be consistent with the requirements of <organization name>'s Event Log Management and Monitoring Standard.

4-6	Proxy logs must include at least the following information: ● date and time of session ● source IP address ● user login ● destination IP ● action performed ● full URL path ● categorization of URL ● used traffic policy
4-7	Proxy server must be configured to send only specific logs to central log system using syslog protocol and CEF, LEEF or RFC 5425 specified log format.

Table A – Proxy deployment methodologies

Methodology	Description
Inline	Inline deployment is commonly used in small organizations due to the ease of deployment and the absolute security level it provides. With an inline deployment, the web gateway is placed directly in the path of all network traffic going to and from the Internet. If you choose an inline deployment, make sure your web gateway is capable of bypassing network traffic that you don't want processed by the web gateway. In many instances, you can choose to either "proxy" (re-route) or "bypass" a specific protocol. If you "proxy" the protocol, it means the web gateway will terminate the traffic from the client to the server locally and re-establish a new connection acting as the client to the server to get the requested information.
Explicit	Explicit deployment is commonly used when a web gateway is deployed in a larger network, and the design of the network requires there to be no single point of failure. Explicit deployment allows the web gateway to be located on the network in any location that is accessible by all users and the device itself has access to the Internet. Explicit deployment uses an explicit definition in a web browser. To facilitate this kind of deployment an administrator can distribute PAC or WPAD files for the explicit proxy setup in end-user browsers.
Transparent	Transparent deployment allows a web gateway to be deployed in any network location that has connectivity, similarly to explicit mode deployment, reducing the need for a

	configuration change to the network to implement. In addition, there is no administrative overhead to configure end-user systems, since the routing of HTTP and HTTPS traffic is typically done by the router or other network device. Transparent deployment is often used when an organization is too large for an inline deployment and does not want the added work and overhead needed for an explicit deployment. Most transparent deployments rely on web Caching Communications Protocol (WCCP), a protocol supported by many network devices. Alternatively, transparent deployment can be achieved using Policy Based Routing (PBR) or usage of application delivery controllers.
Span	SPAN (Switched Port Analyzer) port deployment is sometimes called TCP Reset deployment, as it relies on TCP resets to implement the policy of the web gateway. A web gateway is deployed by attaching it to a SPAN port on a switch. Unlike the other three deployment methods, which process the web traffic and implement policies based on the network response to the web gateway issues, a web gateway deployed on a SPAN port implements policies by issuing a TCP reset to the client system to prevent completing a download of offending content.
Reverse	A reverse proxy is commonly deployed as a server that sits in front of one or more web servers, intercepting requests from clients. This is different from a forward proxy, where the proxy sits in front of the clients. Reverse proxy forwards client (e.g., web browser) requests to web servers. Reverse proxies are typically implemented to help increase security,

	performance, and reliability (e.g., to avoid state or institutional browsing restrictions, to block access to certain content or to protect identity online)

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <information technology function>

4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.