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 outlined image.

Web Application Protection Policy Template

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.

Choose Classification

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

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 policy aims to define the detailed cybersecurity requirements related to the protection of <organization name>'s external web applications to minimize the cybersecurity risks resulting from internal and external threats and to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements such as Essential Cybersecurity Controls (ECC-1:2018) and Critical Systems Cybersecurity Controls (CSCC-1:2019) that are issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all <organization name>'s external web applications and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1- General Requirements

1-1 External web applications must be protected by a web application firewall (WAF) from external attacks.

1-2 External web applications must follow the (Multi-tier Architecture) principle, with at least (2-tier Architecture).

1-3 Critical external web applications must adopt and follow the (Multi-tier Architecture) principle, with at least (3-tier Architecture).

1-4 Only secure communication protocols (such as HTTPS, SFTP, TLS, etc.) must be used.

1-5 Development Environment and Testing Environment must be logically isolated from Production Environment.

1-6 Data and Information Protection techniques must be used in external web applications as per <organization name> approved Data and Information Protection Policy and Classification Policy.

1-7 Web applications purchased from third party vendors must adhere to <organization name>'s cybersecurity policies and standards.

1-8 Minimum web applications and protection standards (OWASP Top Ten Web Application Security Risks) must be implemented for external web applications and critical systems.

1-9 Minimum application programming interface security standards (OWASP Top Ten API Security) must be implemented for external web applications of critical systems.

1-10 Web application cybersecurity architecture requirements must be defined to ensure that the web applications are designed and deployed in a secure manner.

1-11 It must be ensured that all web application event logs in <organization name> can be monitored and stored.

1-12 Integrity, availability and recoverability of web applications data against tampering, accidental loss or damages must be ensured through Backup and Archival.

1-13 Cybersecurity requirements for cloud-hosted web applications must be defined to ensure they are configured, installed and operated in a secure manner.

1-14 External web applications must be available and protected against Distributed Denial of Service "DDoS" Attacks at the applications and network level.

1-15 Procedures and standards for web applications protection must be developed based on business need.

1-16 KPI must be used to ensure the continuous improvement and effective and efficient use of the Web Applications Protection requirements.

2- Access Right

2-1 Multi-factor Authentication must be implemented for user access to external web applications and system admins access to internal web applications.

2-2 Web applications development security standards, including but not limited to Secure Session Management, session authenticity, session lockout, and session timeout, must be documented and approved.

2-3 Access to production systems must be restricted and controlled as per job responsibilities.

2-4 External web application users must be forewarned and acquainted of the Secure Usage Policy.

2-5 Secure means (Hashing Function) must be used to store user data when accessing external web applications such as a password.

3- Security Configuration

3-1 Cybersecurity Risk Assessments must be performed when planning the development or purchase of web applications prior to their deployment in production environment as per <organization name>'s Cybersecurity Risk Management Policy.

3-2 Web application secure configuration and hardening requirements must be defined, reviewed and documented to ensure that the web applications are configured and operated in a secure manner.

3-3 Ensure confidentiality and integrity of web applications data as per <organization name>'s Data and Information Protection Policy.

3-4 Prior to using classified information in testing environment, <cybersecurity function>’s prior authorization must be obtained and restrict controls to protect such data, e.g. data scrambling and data masking, must be used and such data must be wiped immediately after that.

3-5 Source Code must be safeguarded and access to it or modification must be restricted to authorized users.

3-6 External web applications must undergo a Penetration Test in testing environment, results must be documented, and all vulnerabilities must be remediated before deployment in production environment as per <organization name>'s Penetration Testing Policy.

3-7 Vulnerabilities Assessment must be performed for technology components of web applications and vulnerabilities must be remediated by installing <organization name>’s patches on a regular basis.

3-8 Tests must be conducted to asses Web applications protection in case of a new or Major Application Release, Acquired Web Applications, Point Releases, Patch Releases, and Emergency Releases.

3-9 Changes to web applications must be approved by the <Change Advisory Board> (CAB) before being launched into the production environment.

Roles and Responsibilities

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

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

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

4- **Policy 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 policy on a regular basis.

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

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