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

Insert organization logo by clicking on the outlined image.

Web Application Security Standard 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 standard aims to define the detailed cybersecurity requirements related to protecting <organization name> external web applications to minimize cybersecurity risks and protect it against internal and external threats.

These requirements are aligned with the Web Application Protection Policy and NCA's cybersecurity requirements including but not limited to: ECC – 1:2018, CSCC – 1: 2019) and other relevant legal and regulatory requirements.

Scope

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

Standards

1	Access Management
Objective	To ensure the protection of web applications against unauthorized access.
Risk Implication	Unauthorized access to web applications has severe implications that could lead to information exfiltration or theft where they can be used to carry out further cyber-attacks against <organization name>'s infrastructure.
Requirements	
1-1	Secure access and identity management for web applications must be implemented in accordance with the technical security controls mentioned in the Identity and Access Management standard controls applied in <organization name> in order to defend cybersecurity attacks.
1-2	Ensure secure session management, including session authenticity, session lockout and session timeout.
2	Web Application Architecture

Objective	To define web application cybersecurity architecture requirements to ensure that the web applications are designed and deployed in a secure manner.
Risk Implication	Weak security designs are critical security risks that could be exploited in cyber-attacks to jeopardize <organization name>'s business operation
Requirements	
2-1	Web applications for critical systems must follow the multi-tier architecture principle with minimum 3 tiers, or micro-services architecture protected by a dual layer of firewalls must be implemented. More specifically, **webservers** must be placed in the Internet DMZ, **web application servers** must be placed in the Production Zone, and **database servers** must be placed in the Trusted/Database zone.
2-2	Logical or physical isolation of critical web applications from other web applications or systems must be implemented. For example, physical isolation can be achieved by hosting web applications in a completely different separate physical environment, while logical isolation can be achieved by implementing web applications in a separate zone inside the network without allowing access from any other zone.
2-3	Production web applications must be logically isolated from test and development environments using network restrictions by configuring Access-Control Lists (ACLs) and security policies on firewalls.
2-4	Network access to web applications must be restricted to web servers zones, web applications server zones and management server zone.
2-5	A Web Application Firewall (WAF) must be deployed in front of all web application servers to verify and validate the traffic going to the server. Since WAF devices detect or block web-

	based and application-based attacks on external-facing services and web applications, any unauthorized traffic must be blocked and logged. (Additionally, WAF must be configured to enable IP the intelligence feature and IP geo-location features in order to block blacklisted IPs and specific countries).
2-6	Configure WAF to mitigate OWASP Top Ten Web Application Security Risks for critical web applications as per <organization name>'s relevant standard controls.
2-7	Apply API security controls to mitigate OWASP Top Ten API Security for critical web applications at the minimum level.
2-8	IPS and WAF must be configured to enable signatures that match the web application behavior and protocols (e.g., Oracle OHS, IIS, Apache, SQL, XML, etc.).
2-9	Malware protection solution and APT systems must be configured to check all file transfer operations related to web applications for malicious files for example as per <organization name>'s Malware Protection Policy and Standard controls.
2-10	Web application security solutions and systems must be configured to follow a positive security model or whitelisting model by allowing only specific file types, specific protocols and ports, specific layer 7 web applications and specific web application parameters, while denying all files and applications that are not configured.
2-11	Secure web applications and communication protocols, such as HTTPS, SFTP, TLS, etc. must be used.
3	Secure Configuration and Hardening

Objective	To define web application secure configuration and hardening requirements to ensure that the web applications are configured and operated in a secure manner.
Risk Implication	Misconfiguration and weak configurations of web applications and its technology components are common security vulnerabilities that could be exploited in cyber-attacks to jeopardize <organization name>'s business operation
Requirements	
3-1	Secure configuration and hardening for web applications must be implemented in accordance with the technical security controls mentioned in the Secure Configuration and Hardening standard controls applied in <organization name> in order to defend cybersecurity attacks.
3-2	Web application security assessments, including Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), must be performed regularly.
3-3	Unnecessary/unrequired services, functionalities and configuration files must be removed or disabled.
3-4	Access to unnecessary/unrequired network shared files and directories must be blocked.
3-5	Application source code must be secured and hardened.
3-6	Secure web application images or templates must be created for all web applications based on the approved configuration standard controls. Any web application server that becomes compromised must be reimaged using one of these image templates.
3-7	Images must be stored in a secure environment on securely configured servers, and must be regularly validated using integrity monitoring tools.

4	Availability
Objective	To maintain availability of external web applications against denial of service attacks (DDOS) and accidental failure.
Risk Implication	If web applications are not sufficiently protected against denial of service attacks and infrastructure failure, web applications could be a target of DoS attacks and face sustained service outage and performance issues.
Requirements	
4-1	A web application architecture that eliminates the existence of single points of failure must be deployed and implemented.
4-2	Load balancing mechanisms, such as those offered by an application load balancer device, must be deployed.
4-3	Web application data replication mechanisms must be implemented on Disaster Recovery (DR) or secondary sites.
4-4	An exact replica of critical web application production environment must be deployed on the Disaster Recovery (DR) site.
4-5	For web applications hosted by third parties, the Service Level Agreement (SLA) must maintain an acceptable level of web application and services availability in accordance with <organization name>'s Third Party Cybersecurity Policy.
4-6	Automated or manual web application traffic redirection to the backup or Disaster Recovery (DR) site must be configured in case of production environment failure.
5	Cryptography
Objective	To ensure the confidentiality of web application data and verify its integrity.

Risk Implication	Without encryption and integrity validation techniques, web application data and protected information could be exposed, tampered or accessed without authorization.
Requirements	
5-1	Cryptography for web applications must be implemented in accordance with the technical security controls mentioned in the Cryptography standard controls applied in <organization name> and related laws and regulations in order to defend cybersecurity attacks.
5-2	End-to-end encryption for web applications client/server communications must be used.
5-3	Web application certificates must be provided from a trusted CA compliance source and periodically renewed in accordance with the related laws and regulations.
5-4	Certificate based asymmetric (private/public) cryptography must be used for all public external web applications as per <organization name>'s Cryptography Standard controls.
5-5	Encryption functionalities and certificate management must be enabled on the web application firewall to provide more visibility into threats and attacks.
5-6	Web applications cryptographic keys must be stored in a secure vault and physically secure locations as per <organization name>'s relevant policies and procedures.
6	Event and Audit Logging
Objective	To ensure all web application events in <organization name> are monitored and logged.

Risk Implication	Failure to monitor and log web application events in <organization name> will make it difficult for it to detect cybersecurity attacks and threats, leading to more damages to the applications.
Requirements	
6-1	Event and Audit Logging for web applications must be enabled in accordance with the technical security controls mentioned in the <organization name>'s Cybersecurity Event Logs and Monitoring Management standard controls in order to defend cybersecurity attacks.
7	Backup and Archival
Objective	To ensure the integrity, availability and recoverability of web application data against tampering, accidental loss or destruction.
Risk Implication	If web applications data are deleted or tampered due to accidental loss, damage or attack the <organization name> will not be able to recover data which will impact normal business operations .
Requirements	
7-1	Backup and archival for web applications must be implemented in accordance with the technical security controls mentioned in the Backup and Recovery Management standard controls applied in <organization name> in order to defend cybersecurity attacks.
7-2	Full backups for web applications must be performed, serialized, time-dated and indexed in accordance with <organization name>'s Backup and Recovery Management Policy. The backups must include at minimum web

	applications' configuration backups, and the stored data and information of web applications.
8	Modernized and Cloud Native Web Applications
Objective	To define cybersecurity requirements for cloud native web applications to ensure that they are deployed, configured and operated in a secure manner.
Risk Implication	Using cloud computing service to operate web applications without proper security and cybersecurity measures are common security vulnerabilities that could be exploited in cyber-attacks to jeopardize <organization name>'s business operation efficiency .
Requirements	
8-1	A DevSecOps methodology and process must be developed and adopted.
8-2	A secure Continuous Integration/Continuous Deployment (CI/CD) pipeline must be developed and implemented following best practices.
8-3	A container security platform must be deployed from a trusted vendor to manage container security and ensure that the container system is safe.
8-4	Security patches must be regularly deployed.
8-5	Critical information management mechanisms must be implemented to manage Confidential information, keys and certifications, and prevent storing confidential information in containers.
8-6	Container images from trusted or approved sources must be used.
8-7	Containers' infrastructure must be isolated.

8-8	Automated vulnerability detection must be used to scan containers before and after their deployment into the production environment.
8-9	Monitoring tools must be deployed to regularly monitor applications' health, availability, and efficiency.

Roles and Responsibilities

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

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

3- **Standard Implementation and Execution:** < IT function> and <cybersecurity 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 standards may be subject to disciplinary action according to <organization name>'s procedures.