WEBSITE SECURITY POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	WEBSITE SECURITY POLICY
Document Number:	COS/POL/12
Version:	1.0
Document Date:	17-06-2026
Prepared By:	HOD-IT
Reviewed By:	CISO
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Review Date	Version No.
1	Initial Basic Release	**17-06-2026**	1.0

Contents

1. PURPOSE

The purpose of this Policy is to establish a consistent framework for protecting the websites, web applications, APIs and supporting infrastructure of LLP against cyber threats, unauthorized access, data breaches and operational disruptions. It defines the minimum-security requirements for the secure design, development, deployment, operation, maintenance and retirement of organizational websites while supporting compliance with applicable legal, contractual and information security obligations.

2. SCOPE

- This Policy applies to all websites, portals, web applications, APIs, cloud-hosted environments, supporting infrastructure, databases, content management systems, Domain Name System (DNS) services and associated technologies owned, operated, or managed by LLP or its authorized service providers.
- The Policy is applicable to all employees, website owners, IT administrators, developers, contractors, consultants, cloud providers, hosting agencies, maintenance vendors, and third parties involved in website operations.

3. WEBSITE SECURITY REQUIREMENTS

a) Website Hosting and Infrastructure Security

Website infrastructure shall be deployed and maintained using secure architecture and industry-recognized security practices. Appropriate physical, logical, and environmental controls shall be implemented to protect organizational assets from unauthorized access, cyber threats, equipment failures, and environmental risks. The organization shall ensure:

- Physical access to critical infrastructure is restricted to authorized personnel.
- Servers and hosting environments are securely configured and hardened before deployment.
- Development, testing, staging, and production environments remain segregated.
- Default accounts, unnecessary services, and insecure configurations are removed.
- Operating systems, applications, and infrastructure components are regularly updated with approved security patches.
- Secure communication protocols, firewalls, network segmentation, intrusion detection, VPN access, and encryption mechanisms are implemented where appropriate.
- Backup power, monitoring, and disaster recovery capabilities are maintained to support business continuity.

b) Website Development and Secure Configuration

Security shall be incorporated throughout the Software Development Life Cycle (SDLC) to minimize vulnerabilities and ensure secure deployment of websites and applications. The organization shall ensure that:

- Domain registration, SSL certificates, and DNS services are centrally managed and periodically reviewed.
- Website information is classified based on business sensitivity, and appropriate protection measures are applied.
- Secure coding practices and recognized industry standards such as OWASP are followed during application development.
- Source code undergoes peer review, security testing, vulnerability assessment, and penetration testing before production deployment.
- Servers are securely configured using approved security baselines, and administrative access is restricted to authorized personnel using strong authentication and, wherever feasible, Multi-Factor Authentication (MFA).
- Access privileges are granted according to the principles of least privilege and need-to-know, with periodic access reviews and timely revocation of obsolete accounts.
- Regular backups of websites, databases, source code, and configurations are performed, securely stored, encrypted where necessary, and periodically tested to ensure successful recovery.

4. WEBSITE OPERATIONS AND SECURITY MONITORING

Website security shall be continuously monitored throughout the operational lifecycle to ensure the confidentiality, integrity, and availability of organizational services. LLP shall maintain processes for:

- Continuous monitoring of websites, servers, APIs, databases, and supporting infrastructure.
- Detection of unauthorized activities, suspicious events, malware infections, configuration changes, and service disruptions.
- Periodic Vulnerability Assessments and Penetration Testing (VAPT) based on business risk.
- Timely remediation of identified vulnerabilities according to their severity.
- Secure maintenance of audit logs to support monitoring, investigations, and compliance activities.
- Regular compliance reviews, internal audits, security assessments, and technology lifecycle management.
- Controlled website content management to ensure only approved, accurate, and authorized information is published.

- Planned maintenance, software upgrades, certificate renewals and secure decommissioning of obsolete websites and supporting infrastructure.

5. CHANGE MANAGEMENT

- All changes affecting website infrastructure, applications, databases, APIs, or supporting services shall follow a formal Change Management process.
- Significant changes shall be documented, risk assessed, approved, tested in non-production environments, and implemented using appropriate rollback procedures. Emergency changes shall be documented and reviewed after implementation, while segregation of duties shall be maintained between development, testing, approval, and deployment activities wherever practicable.

6. SECURITY INCIDENT MANAGEMENT

- LLP shall maintain a structured incident management process to ensure that website-related security incidents are promptly identified, reported, investigated, contained, resolved, and documented.
- Security incidents may include unauthorized access, website defacement, malware infections, denial-of-service attacks, data breaches, credential compromise, DNS manipulation, or any activity affecting website confidentiality, integrity or availability.
- The organization shall ensure that incidents are appropriately classified, investigated, supported by forensic evidence where necessary, and followed by corrective and preventive actions. Incident records shall be maintained, and relevant stakeholders or regulatory authorities shall be notified where legally or contractually required.

7. VENDOR SECURITY

- Third-party organizations involved in website hosting, development, maintenance, cloud services, or infrastructure support shall comply with the organization's security requirements.
- Vendor agreements shall include appropriate provisions relating to confidentiality, data protection, secure development, incident reporting, vulnerability management, access control, audit rights, business continuity, and secure handling of organizational information.
- Third-party access shall be approved, periodically reviewed, monitored, and revoked immediately when no longer required.

8. ROLES AND RESPONSIBILITIES

- Management shall provide oversight and resources necessary for implementing this Policy.
- Website Owners shall ensure compliance with security requirements, approve website content and changes, and oversee remediation of identified risks.
- The Information Security function shall maintain this Policy, coordinate security assessments, monitor compliance, and manage incident response activities.
- IT Administrators and Developers shall implement secure configurations, maintain infrastructure, perform security testing, apply updates, manage backups, and support continuous monitoring.
- Employees and third-party personnel shall protect organizational information, comply with approved security procedures, safeguard authentication credentials, and promptly report suspected security incidents.

9. COMPLIANCE

- Compliance with this Policy shall be verified through periodic audits, vulnerability assessments, security reviews, and management oversight. Any non-compliance shall be documented, risk assessed, and addressed through appropriate corrective actions.

10. EXCEPTIONS AND POLICY REVIEW

- Exceptions to this Policy shall require documented business justification, risk assessment, compensating controls, management approval, and periodic review.
- Policy shall be reviewed at least annually or whenever significant changes occur in technology, regulatory requirements, cybersecurity threats, or business operations to ensure its continued effectiveness and alignment with organizational objectives.