حكومة دبي
GOVERNMENT OF DUBAI

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

Web Security Policy

VERSION 1.0

GOVERNMENT OF DUBAI

WEB SECURITY POLICY

VERSION 1.0

TABLE OF CONTENTS

INTRODUCTION

Developments are nowadays not happening anymore in isolation; the macro trend is to have interconnected web- and API-based developments. Observing these trends and statistics in cyber security, there is an obvious observation to make: new web-based attack types and vectors are coming out every day, causing organizations, communities and individuals to take security seriously now more than they ever have in the past. Robust and securely developed web sites, web applications and mobile applications increase the cyber security and cyber resilience tremendously. This Web Security Policy has been developed to support Dubai governments to achieve high levels of the cyber security and cyber resilience.

Modern development has many challenges, and cyber security does not always get the right emphasis during the development phase. This Web Security Policy is highlighting the principles of web security that any organization or developer should follow, with the intent to help Dubai governments to achieve more holistic cyber security.

The fundamentally important cyber security standard listed in the Information Security Regulation (ISR V2) has already broached the issue of secure development and web security, and this policy was developed to support the important aspect of web security in the overall ISR implementation (for more detail, please refer to Clause 2).

This Web Security Policy and its supporting guidelines have been developed to support Dubai governments in managing the important, yet complex space of web security successfully.

.

1 EXECUTIVE SUMMARY

1. EXECUTIVE SUMMARY

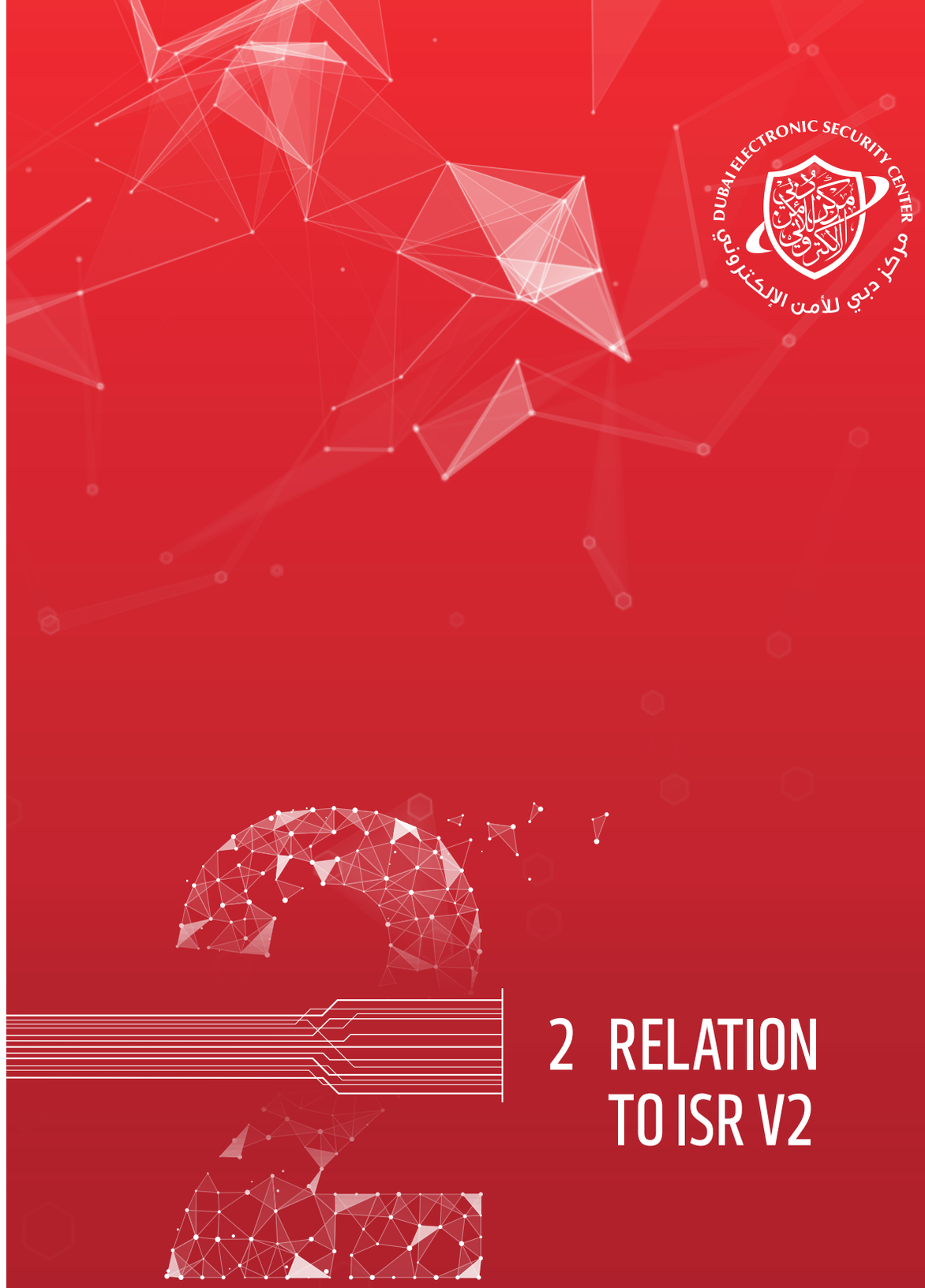
This Web Security Policy has been developed to support Dubai's government in achieving higher levels of security when developing and using web applications and services. Web security is based on the well accepted thoughts of application security, but is applying those specifically to the fundamental elements:

- WEB SITE SECURITY
- SECURITY OF WEB APPLICATIONS
- SECURITY OF MOBILE APPLICATIONS
- API SECURITY

The use of the internet, web sites, web applications, mobile applications and APIs (Application Programming Interfaces) has been vastly increasing throughout the years, making web security an immanent topic to be addressed successfully for any organization wishing to use such services.

Implementation of this Web Security Policy and its supporting guidelines forms an important part of the implementation of Dubai's Cyber Security Strategy, and compliance with this policy is mandatory for all Dubai governments; requirements are denoted by "shall" statements.

Compliance with this Web Security Policy will be audited by DESC, in combination with the ISR audit or separately.



2 RELATION TO ISR V2

2. RELATION TO ISR V2

Several topics related to web security, such as public information, application development, secure coding standards and security testing have already been addressed in ISR V2, in the Sub-Controls 6.7.2, 8.1.1 and 8.1.2, and also in the Main Controls 7.4, 8.2 and 8.6. These controls shall be completely implemented by all elements (see Section 1) of this Web Security Policy.

The purpose of this Web Security Policy is to elaborate on the different ISR topics related to web security, and to provide further information about how higher levels of web security can be achieved. This will be supported by further detailed guidelines, which will help to implement this policy.

It is important to address other information security topics, such as acceptable user behaviour or good password selection by complying with ISR V2, as only a holistic approach provides reliable security. In addition, it shall be ensured that any sensitive data, on web sites, web applications, mobile applications or APIs, is stored and processed in the UAE; this shall also be the case if clouds are used.

3 WEB SECURITY ELEMENTS

3. WEB SECURITY ELEMENTS

There are different scenarios that need to be considered when addressing security in web sites, web applications, mobile applications and APIs:

- In-house development
- Outsourced development
- Procurement of solutions
- Existing and legacy solutions

3.1 In-House Development

3.1.1 Whenever a web site, web application, mobile application or API is developed in-house (with in-house talent or the help of hired developers), it shall be ensured that all relevant requirements in Section 4 are complied with.

3.1.2 A person responsible for the development (process or business owner) shall be identified and this shall be documented, e.g. in the information asset register (see also ISR V2 Main Control 2.1).

3.1.3 Security and privacy requirements that the development needs to fulfill shall be identified and documented.

3.1.4 Developers shall develop code using a low privileged account. Deployments during all phases of the lifecycle of the application shall run under this account.

3.1.5 All events related to major changes shall be logged, in compliance with ISR V2 Main Control 8.5.

3.1.6 All ISR V2 controls related to risk management and classification shall be applied to the development.

3.2 Outsourced Development

3.2.1 Whenever outsourced development of a web site, web application of mobile application is used, it shall be ensured (for example contractually) that all relevant requirements in Section 4 are complied with.

3.2.2 A person responsible for managing the outsourced development shall be identified and this shall be documented, e.g. in the information asset register (see also ISR V2 Main Control 2.1).

3.2.3 Security and privacy requirements that the development needs to fulfill shall be identified and documented, and their fulfillment included in the outsourcing contract.

3.2.4 The outsourcing contract shall include the right to audit.

3.2.5 Where possible, application source code shall be owned.

3.3 Procurement of Solutions

3.3.1 Whenever a solution for a web site, web application of mobile application is procured, it shall be ensured that the product fulfills all relevant requirements in Section 4.

3.3.2 A person responsible for the purchased solution shall be identified and this shall be documented, e.g. in the information asset register (see also ISR V2 Main Control 2.1).

3.3.3 Security and privacy requirements of the solution procured needs to fulfill shall be identified and documented, and their fulfillment ensured before purchasing.

3.3.4 Any existing or legacy solution for a web site, web application or mobile application shall fulfill all relevant requirements in Section 4. If this is not the case, a risk assessment shall be conducted, and mitigating controls applied. The results of this risk assessment shall be documented.

3.4 Existing and Legacy Solutions

3.4.1 Any existing or legacy solution for a web site, web application or mobile application shall fulfill all relevant requirements in Section 4. If this is not the case, a risk assessment shall be conducted, and mitigating controls applied. The results of this risk assessment shall be documented.

3.4.2 Security and privacy requirements that the existing or legacy solution needs to fulfill shall be identified and documented, and their fulfillment ensured before continuing its operation.

4 REQUIREMENTS FOR WEB SECURITY

4. REQUIREMENTS FOR WEB SECURITY

All requirements denoted by * apply only for the development of web applications, mobile applications and APIs.

4.1 Secure Sessions

4.1.1 * Unique session IDs shall be generated by the server and sent to the client. The frequency of session ID generation and what is allowed to be performed for the same user ID can be determined by the risk assessment results. Sufficiently long keys shall be used, and it shall be possible to invalidate the session ID at any time.

4.1.2 * Server-side sessions shall be invalidated upon logout.

4.1.3 * Session IDs shall be suitably random as determined by the results of the risk assessment.

4.1.4 Cookies shall not be used to obtain sensitive, private or confidential information, users shall be made aware of the fact that cookies are used, and users shall be able to delete cookies, if wanted.

4.1.5 Cookie attributes shall be set to known prevent attacks and it shall be ensured that cookies have a maximum age or expire; the latter is depending on the results of the risk assessment.

4.1.6 Third party cookies shall be evaluated before being allowed to be used for web sites and applications.

4.1.7 Unless required, cookies associated with subdomains shall be stored at subdomain level.

4.2 Encryption

4.2.1 * Where, based on the results of the risk assessment, confidentiality is required, sessions shall be encrypted, and session IDs shall be randomly assigned.

4.2.2 * The login session shall be encrypted using TLS[1] (other types on encryption can be used in case of higher security requirements, as per the risk assessment results). Obsolete or vulnerable sessions being prone to security downgrades shall not be used.

4.2.3 SSL/HTTPS access to all pages shall be enforced, and any links on sites shall be HTTPS links. If higher levels of security are required based on the results of the risk assessment, at minimum TLS shall be enforced.

4.2.4 Sensitive logging information shall be identified and well structured, and this information shall be encrypted.

4.2.5 All administrative access to databases via the front-end interfaces shall be encrypted.

4.2.6 Encryption keys used for local data encryption for mobile devices should be stored within the manufacturer's key storage space on this device and should conform to key management policies by the risk assessment.

4.3 Identity Management

4.3.1 Access to sites, services or applications shall be given based on defined user identities and the associated job role.

4.3.2 The use of external non-government identity providers shall be avoided, where possible.

4.3.3 User IDs shall not be incremented.

4.4 Authentication

4.4.1 The ISR V2 requirements for secure password selection shall be applied and passwords shall be managed securely. Other authentication mechanisms shall be used on the basis of the results of the risk assessment.

[1] Please note: in case of legacy systems not being capable of using TLS, refer to Section 3.4 and ensure that these requirements are fulfilled.

4.4.2 How a consecutive number of defined failed login attempts are dealt with shall be determined based on the risk assessment results; examples are: blocking the account or raising an alert after a defined number of attempts.

4.4.3 User shall be sent an email at the pre-registered email address if his/her account is locked.

4.4.4 Login error messages shall be generic in nature to prevent user ID enumeration.

4.4.5 Multifactor authentication shall be used whenever the risk assessment results demand higher levels of security.

4.4.6 CAPTCHA or HIP controls shall be implemented on the login page to prevent brute force attacks.

4.5 Authorization/Access Control

4.5.1 * Least privilege access shall be applied; this shall also apply for developers.

4.5.2 Authorization controls shall be enforced on every request to the application or site.

4.5.3 Authorization to access any resource (including files, protected URLs, protected functions, services and application data) shall be verified prior to granting access to that resource. Only trusted resources shall be accessed.

4.5.4 Authorization controls shall be enforced on every request, including those made by server-side scripts and requests from technologies like AJAX.

4.5.5 Cross-Origin Resource Sharing (CORS) implementation shall follow strict rules of allowing only authorized nodes to access the resources.

4.5.6 Access by external parties such as (developers, system engineers, support) shall not be granted on production servers. If such access is necessary, it shall only be provided temporarily through monitored means.

4.5.7 Regular access review shall be conducted on application's resources, including but not limited to remote access and administration consoles.

4.6 Input Validation

4.6.1 Input, headers and cookies shall be validated before it goes into execution or being parsed by servers.

4.6.2 All data shall be encoded with a common character set prior to validation.

4.6.3 Whitelisting (for allowed characters) and blacklisting (of potentially hazardous characters) shall be used.

4.6.4 All input shall be validated to ensure there has been no client-side attacks which could include XSS, HTML injection, or any attacks which could compromise the end user.

4.6.5 Buffer overflow shall be prevented by defining reasonable field lengths, specific data types, input termination, and prevention of format string attacks.

4.7 Site Configuration

4.7.1 All services, ports and accounts unnecessary for the actions carried out shall be disabled.

4.7.2 Only recommended certificates shall be used; self-signed certificates shall not be used.

4.7.3 The debugging function shall be disabled.

4.7.4 Version numbers or details that may lead to the discovery of vulnerabilities shall not be exposed.

4.7.5 Web configuration files (where applicable) shall be encrypted and any server-side configuration files shall have proper access permissions.

4.7.6 Critical applications shall not be run on shared hosting or on weak web application containerization.

4.7.7 Webserver processes shall run under a non-privileged user ID.

4.8 Logging

4.8.1 All authentication and authorization activities shall be logged; the Main Control 6.9 in ISR V2 shall be complied with.

4.8.2 Access to databases for all user types shall be logged.

4.8.3 Logs shall not contain any confidential or private information (such as passwords or personally identifiable information).

4.8.4 Logs shall be kept for at least 6 months, and at least as long as the results of the risk assessment determine.

4.8.5 The level of logging shall be determined by the risk assessment.

4.9 Error Handling

4.9.1 Error handling shall be tested; sensitive information shall not be displayed on error pages, and generic error pages and global handlers are used to catch unhandled exceptions.

4.9.2 Error messages shall not include the nature of the error.

4.9.3 Custom generated error message shall not indicate the cause of the problem, such as an incorrect user name or password.

4.10 Data storage

4.10.1 The server shall not save passwords in clear text.

4.10.2 Database ports shall not be exposed.

4.10.3 Databases shall not allow root access or be run with root privileges.

4.10.4 Database content shall be encrypted based on the results of the risk assessment; in case of credit card data being contained in a database, compliance with PCI DSS v3.2.1 shall be achieved.

4.10.5 Uploaded and stored files, including the directory in which it was stored, shall not be accessible through the interface they were uploaded.

4.10.6 Uploaded files shall not preserve their names and the new name shall not be guessable, nor using configuration type file names. In addition, file names shall follow documented conventions.

4.10.7 For stored files, no file path shall be revealed to a user.

4.10.8 The storage directory shall not allow executable files to be executed.

4.10.9 It shall be ensured that the uploaded file is valid based on the stated file extension, the checked mime type, the verified content type, and that it is within the range of allowed file types and sizes.

4.11 Hosting Server

4.11.1 The hosting server shall not return more information than requested.

4.11.2 It shall be ensured that the hosting server's operating system has the latest updates, patches and service packs.

4.11.3 Hosted application files shall be protected and have specific permissions based on business requirements.

4.11.4 All unnecessary files, such as sample website files, test files, unnecessary application files, backups, or development tools from the production servers shall be removed from the hosting server.

4.11.5 Web root folder shall be situated on a different file system from the operating system and directory traversal shall be disabled; files and folders not necessary for operation shall not be placed in the Web root folder.

4.11.6 Default administrator accounts for applications and databases shall be disabled and replaced by a non-privileged administrator account.

4.11.7 Developers shall not allow plain text storage of system passwords.

4.11.8 Clear text remote access services such as telnet shall be disabled and secure methods such as SSHv2 shall be used.

4.11.9 Based on the results of the risk assessment, a web application firewall shall be in place for the hosting server.

4.11.10 Plans on how to manage DDoS attacks shall be developed and documented.

4.11.11 The hosting server shall expose only the required ports and shall not include any unnecessary modules.

4.11.12 The hosting server shall allow administrator access only within their network.

4.11.13 Classified data on the hosting server shall reside within the geographical boundaries of the UAE.

4.12 Client Storage

4.12.1 The username and password and any other user information shall not be stored on the user machine.

4.13 Third party libraries

4.13.1 Applications shall use libraries from trustworthy sources, use agreed upon versions of libraries, and all security patches shall be installed.

4.13.2 Developer shall be aware of deprecated libraries and shall ensure that they are not used. A process for monitoring and updating of libraries shall be in place.

4.13.3 Third party libraries shall not connect to their origin or make any other unauthorized connections.

4.14 Mobile Device Security

4.14.1 Text fields that have sensitive inputs such as passwords shall be used with the security options provided by that device.

4.14.2 Depending on the risk level assessed for the application, appropriate procedures shall be in place to manage access for jailbroke devices.

4.15 Miscellaneous

4.15.1 Code in production shall not include any unnecessary or commented out code; comments shall not contain any sensitive information.

4.15.2 All software codes and developments shall contain comments and documentation throughout the code.

4.15.3 * Applications shall have a low-level diagram and high-level diagram of their architecture and data flow. Documentation on the application and database structure shall be created.

4.15.4 Flash shall not be used.

4.15.5 Proper SSL certificates shall be pinned on the mobile devices.

4.15.6 Checks shall be made to detect rooted devices.

4.15.7 Screen caching shall be disabled for mobile devices.

4.15.8 DESC Public Key Infrastructure is the trusted government certificate provider. DESC Public Key Infrastructure certificates shall be used where applicable.

4.15.9 Penetration testing shall be carried out for each version of the application or site, and also after corrections have been made that are not leading to new version numbers.

4.15.10 If chatbots are used, they shall not have access to the organization's systems and shall use encrypted channels. Storage of sensitive and private information collected through chatbots shall be done based on a risk assessment.

4.15.11 * Machine learning and AI models used in the application shall not be directly accessible by the user.

4.15.12 Projects containing Blockchain components shall also adhere to the requirement of the Blockchain Policy issued by Smart Dubai Office.

4.15.13 Applications that send out emails shall do so only through a trusted email gateway or server with the necessary email security filters.

4.15.14 Connectivity to email services shall be done through a secure channel and credentials used shall be encrypted.

4.15.15 A backup schedule shall be defined, and it shall be ensured that applications and their data have been successfully backed up (this and the following controls in this clause link to ISR Main Control 7.4).

4.15.16 It shall be ensured that all backups are protected and encrypted.

4.15.17 Periodic audits shall be performed against the backup process and the media to identify successful backups.

4.15.18 Least privilege shall be given to the backup process; the logging shall be enabled and regularly reviewed.