|  |  |
| --- | --- |
| **Walpita Enterprises Pvt Ltd**  **Walpita Enterprises Pvt Ltd,**  **Horana,**  **Sri Lanka.** | **APPROVED BY: ISSC**  **Date:** 03-10-2024 |
| **VERSION NO : 1.0**  **Distribution: Internal** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **By** | **Date** | **Section Affected** | **Reason** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**1.0 Purpose**

The purpose of this policy is to define security controls which required to follow when performing software development activities internally and when acquiring 3rd party systems to solve a business requirement of the Walpita Enterprises Pvt Ltd.

**2.0 Scope**

This policy applies to all employees, contractors, outsourced staff and all other entities working on behalf of the Walpita Enterprises Pvt Ltd, its subsidiaries and associated companies, who are involving in internal software development activities.

**3.0 System Acquisition, Development & Maintenance**

A system acquisition policy is managed by Walpita Enterprises Pvt Ltd and is out of scope for this ISMS.

**3.1 Security Requirements of Information Systems**

**3.1.1 Information Security Requirements Analysis and Specification**

A risk assessment is conducted for every project as per the Information Security in IT Procurement and Supplier Managemenr policy. The output defines the service specification needed to fulfil the requirements of a project.

**3.1.2 Securing Application Services on Public Networks**

All architecture levels (business, data, applications, and technology) have information security built in, balancing the need for security with the need for accessibility. During transmission outside of the trusted research environment, all Confidential or Secure material is safeguarded by risk mitigating procedures such as cryptography.

**3.1.3 Protecting Application Services Transactions**

The following security controls or features set out in in Table are considered for code that will collect and process information, particularly when the data is classified as Confidential or Secure.

|  |  |
| --- | --- |
| **Security Control** | **Description** |
| Authentication | Authentication of systems should perform through the identity provider of the organization along with the ADFS. |
| Access control | The ability to allow only appropriate access to data (such as with file rights, encryption, etc.) based on its sensitivity and who should have access to it. |
| Auditing & logging | The ability to log access attempts (both successful and unsuccessful) at least to privileged areas, or sensitive information. |
| Input/output & data validation | The ability for the application to determine that data entered and received by the user is in an acceptable format and will not compromise the security of the application. |
| Encryption | All information must be encrypted based on the cryptographic policy. |
| Physical | Physical issues including environmental threats such as power failure, physical access to offices, infrastructure and data should all be considered and appropriate features and measures implemented. |

**3.2 Security in Development and Support Processes**

**3.2.1 Secure Development Policy**

This policy applies to anyone who is commissioned to create an application to be used by multiple users for the collection and processing of information. This includes:

1. Installable software packages programmed for use within the Walpita Enterprises Pvt Ltd, virtual or desktop computers.
2. This policy covers only the systems hosted in the Data Center.

**3.2.1.1 Security Principles**

The concepts outlined in the following sections must be followed throughout the software development process. The Open Web Application Security Project (OWASP) website provides a synopsis for each concept, as well as links to other resources.

**3.2.1.2 Apply Defence in Depth**

Layered security mechanisms must be in place to increase security as a whole. Any public facing application should be routed through Web Application Firewall (WAF). The design and development of a public facing application, must be approved by IT Steering Committee (ITSC).

**3.2.1.3 Use a Positive Security Model**

A ‘positive’ security model defines what is allowed and rejects everything else. For example, applications by default disable for all users and grant access based on the requirement. This applies a ‘whitelist’ (positive), rather than ‘blacklist’ approach.

**3.2.1.4 Fail Securely**

Handling errors is a key aspect of secure coding. It is important that failures are handled so that exceptions do not enable behaviour that the countermeasure would not normally allow. For example, application query strings are checked for valid key value pairs - if either is incorrect then a generic error is issued and if the query string sends parameters to the database this process will not be called and a database connection is not established.

**3.2.1.5 Run with Least Privileges**

The principle of least privilege must be followed in order to complete the business process. One example is database connection rights granted by programs. If there are various sets of user groups with varying data access credentials, separate account groups are set up to consistently constrain access. Create a read-only access group for read users and a read/write access group for editor users, for example. To provide such access, however, a clear justification of the business requirement, as well as the completion of an approval process, are required.

**3.2.1.6 Avoid Security by Obscurity**

Security by obscurity is alone a weak security mechanism, however when combined with all principles it can be used as an additional layer of security.

**3.2.1.7 Keep Security Simple**

Attack surface area and simplicity go hand in hand. It is important to keep security simple.

**3.2.1.8 Detect Intrusions**

Collect and record any information regarding access and usage that can assist in detecting and monitoring unauthorised actions.

**3.2.1.9 Don’t Trust Services**

Some applications may refer to external systems or packages when developing, always make sure to use secure external systems or packages when developing applications.

**3.2.2 System Change Control Procedures**

Applications that are developed and hosted internally should be subjected to formal change management process.

**3.2.3 Restrictions on Changes to Software Packages**

The following must be observed with regard to software:

1. All software acquired by the Walpita Enterprises Pvt Ltd must be installed by the ServiceDesk by following a Software request raised in the ServiceDesk system.
2. All software acquired by the Walpita Enterprises Pvt Ltd must perform the security testing before installing in the endpoints, servers etc.
3. Except for backup or archival purposes, copying of any software is expressly prohibited.
4. The use of unlicensed software is not permitted under any circumstances.
5. Personal, programs or utilities may not be installed on any internal servers/endpoints.
6. Only Walpita Enterprises Pvt Ltd can provide and modify infrastructure configuration.

**3.2.4 Secure System Engineering Principles**

Where applications have been developed to collect information across public infrastructure:

1. All traffics must encrypted.
2. Applications must be user acceptance tested and security tested by Walpita Enterprises Pvt Ltd against the OWASP security principles.
3. Critical, high and medium risks must remediate immediately.

**3.2.5 Secure Development Environment**

Walpita Enterprises Pvt Ltd Data Center is a secure environment and Information Security and Compliance team of Walpita Enterprises Pvt Ltd should perform periodic vulnerability assessments on critical network segements and provide identified issues to the Network team to remediate issues. Further, patching systems should be done as per the patch management policy.

**3.2.6 Outsourced Development**

Applications that are developed by a 3rd party should be acquired to the Walpita Enterprises Pvt Ltd based on the procument policy.

**3.2.7 System Security Testing**

Before the application is deployed in the live environment, application security testing must be performed and issues discovered by the security testing must be resolved. This is done to guarantee that any compatibility issues originating from different contexts do not interfere with the application's functionality or introduce new security risks.All applications are tested and validated against the OWASP Secure Coding Practices.

1. Testers must differ from the person(s) who developed the application.
2. Automated systems can be used to test systems.

**3.2.8 System Acceptance Testing**

Required to perform user acceptance testing and obtaining approval for the application before deploying in the live environment.

**3.2.9 Test Data**

Test data should be created for the purposes of developing and testing the application. Testing must not be carried out on live data.

**3.3 The Protection of Test Data**

Ensure there is sufficient test data available to prove the code works and that testing is not performed using live data.

**4.0 Enforcement**

Walpita Enterprises Pvt Ltd reserves the full right to ensure enforcement and compliance of this policy. In the event of violation of the said policy, appropriate corrective and disciplinary action will be taken, up to and including termination of employment.