STAMPEDE DESIGN SDN. BHD.

Information Security Policy

Stampede/ISMS/L1-001-V1.2
Version 1.2
Issued 15th July 2025

0.0 REVISION HISTORY AND APPROVAL

DOCUMENT APPROVAL		
Prepared By:	**Reviewed By:**	**Approved By:**
falihin Nurul Falihin binti Roszaman	Dovlet Nazarov	Nurshazawati Binti Abd Hakim
Date: 09/07/2025	Date: 10/07/2025	Date: 15/07/2025

Version No.	Date	Description
1.0	29/12/2023	Initial Document
1.1	27/05/2024	Updated the following controls requirements based on external audit findings: ● 5.1.23 Information Security for Use of Cloud Services ● 5.4.10 Information Deletion
1.2	15/07/2025	Updated the following in the document based on the current implementation: ● Text formatting and spacing ● Grammatical corrections and refinements ● 5.1.3 Segregation of Duties ● 5.1.11 Return of Assets ● 5.1.23 Information Security for Use of Cloud Services ● 5.3.9 Security of Assets Off-Premises ● 5.4.6 Capacity Management ● 5.4.10 Information Deletion ● 5.4.11. Data Masking

		● 5.4.16 Monitoring Activities ● 5.4.19 Installation of Software on Operational Systems ● 5.4.20 Networks Security ● 5.4.23 Web Filtering

TABLE OF CONTENTS

1.0 INTRODUCTION

i. Stampede recognizes that information is a critical business asset and that its ability to manage, control, and protect this asset will have a direct and significant impact on its future success.

ii. Information should be considered in the broadest sense to include intellectual property, business processes and procedures, marketing, strategic plans, employee, business partner information, finance, human resources, partnerships, and contracts.

iii. Information can be in the form of audio, video, printed or written on paper, magnetic, and stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

iv. Business information must be protected from theft, loss, destruction, unauthorized alteration and unauthorized access. The compromise or loss of business information can have an adverse impact on competitive position and growth, the ability to comply with laws and regulations, and the integrity and trust inherent in Stampede.

v. This Information Security Policy is created to ensure that all employees of Stampede are governed by the importance of protecting data or information which belongs to Stampede. This policy document is created based on International Standard, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

2.0 PURPOSE

i. The objective of this Policy is to provide guidance to strengthen the main component of information security, including the preservation of the Confidentiality, Integrity and Availability of information.

   a. **Confidentiality** – to ensure that relevant systems' information/data is protected with appropriate controls to preserve its confidentiality;

b. **Integrity** – to ensure that all information produced, kept and distributed have absolute integrity;

c. **Availability** – to ensure that systems are always available and operate with minimal disruptions.

3.0 SCOPE

i. This document provides Information security requirements to which all employees and related parties of Stampede are expected to comply, including:

a. All full-time, part-time, and temporary personnel working for Stampede;

b. Contractors and consultants working for or on behalf the Company;

c. All other individuals and groups have been granted access to the information systems and infrastructures.

4.0 DEFINITION

Acronym/Word	**Definition**
Assets	The information assets that shall be protected include, but not limited to information, applications/software, documentations, computing and communication equipment, and supporting utilities.
Asset Owner	Asset owner is the person who is responsible and accountable for the asset. Asset owner may not have property rights to the asset, but has responsibility for its production, development, maintenance, use, disposal and security as appropriate. The asset owner is often the most suitable person to determine the asset’s value for risk assessment purposes.
Availability	Ensuring that authorized users have access to information and associated assets when required.

Acronym/Word	**Definition**
Business Purpose	Any work, job or task that are related to Stampede interests.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Custodian	System/network administrator, system owner, developer or maintainer of a given system, resource or equipment, classified as the following: ● Network Administrator is the custodian of all computing, networking and communication system in Stampede. ● Every individual is the custodian for desktop systems, peripherals and media under their control. ● System Owner is the custodian for specific application software used by Stampede.
Employees	Full time, part time, temporary, seconded and contracted employees of Stampede.
End-user	Users or consumers of a given system, resource or equipment. Also refers to any employee, or third party who is granted access to Stampede IT infrastructure.
External Parties	Trainees, business partners, vendors, suppliers, contractors, external technical support and consultants.
HODs	Head of Departments
Information	Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

Acronym/Word	**Definition**
Information Security	Preservation of confidentiality, integrity and availability of information.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
ISMS	Information Security Management System.
ISMS MR	ISMS Management Representative.
ISWC	ISMS Working Committee.
IT	Information Technology.
OPS	Operations Department.
Security	The state of being free from potential risks/losses related to information in the following categories: ● Information Security ● Information Technology Assets ● Information Technology Resources ● Threats ● Employees ● End-user ● Custodian
Security Baselines	Minimum level of security settings necessary to be implemented throughout Stampede**.**
Teleworking	Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.
Third-parties	Information that is proprietary to a third party, e.g., clients, suppliers/vendors, or former employee of Stampede.
Threats	The potential loss due to deliberate attack, accidents or natural disaster.

5.0 INFORMATION SECURITY POLICY STATEMENTS

5.1 Organisational

5.1.1 Policies for Information Security

i. The Information Security Policy must be defined by ISMS Coordinator and approved by Top Management.

ii. This Policy must be published, communicated to, and acknowledged by employees and relevant external parties through suitable platforms.

iii. This Policy must be reviewed and maintained by ISMS Coordinator at least once a year, or when necessary, in response to any changes affecting the basis of the original risk assessment or in response to requests from within the organisation.

5.1.2 Information Security Roles and Responsibilities

i. Information security within the organisation must be actively supported by Stampede Management through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities and accountabilities.

ii. The identification and assessment of information security risks must be coordinated by ISMS Coordinator in order to define security goals that meet the business requirements.

iii. Information Security responsibilities and functions are formally defined in the Job Description of relevant employee.

iv. Security roles and responsibilities of employees, contractors and third-party users must be defined and documented.

v. All employees of Stampede must be responsible for complying with relevant requirements of the Information Security Policy and associated procedures.

5.1.3 Segregation of Duties

i. As a good practice, the roles with conflicting security requirements must not be assigned to any one individual. Adequate segregation of duties and utmost care must be taken while assigning roles and responsibilities of all key security roles to guard against misuse of systems, data or services whether accidental or deliberate.

ii. Adequate controls must be applied to ensure duties and areas of responsibilities are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of information assets.

iii. Segregation of duties must be maintained for the following roles:

  a. Operations Department

  b. Design Department

  c. Development Department

5.1.4 Management Responsibilities

i. Management must require employees, contractors and third-party users to apply and practice security in accordance with established policies and procedures of Stampede.

5.1.5 Contact with Authorities

i. Appropriate contacts with relevant authorities must be maintained.

5.1.6 Contacts with Special Interest Groups

i. Knowledge and awareness regarding current security threats and security best practices must be proactively maintained by establishing and maintaining relationships with special interest groups, other specialist security forums or professional associations.

5.1.7 Threat Intelligence

i. Information about existing or emerging threats must be collected from external and internal sources, and analysed in order to:

  a. facilitate informed actions to prevent the threats from causing harm to the organisation.

  b. reduce the impact of such threats.

5.1.8 Information Security in Project Management

i. A management authorisation process for new information processing facilities must be defined and implemented.

ii. Information security must be embedded and addressed in every phase of a project lifecycle to ensure the confidentiality, integrity, and availability of data and systems, safeguarding against potential threats and vulnerabilities throughout the project lifecycle.

5.1.9 Inventory of Information and Other Associated Assets

i. All assets must be maintained in an asset inventory.

ii. All information assets associated with information processing facilities must be ‘owned’ by a designated asset owner.

5.1.10 Acceptable Use of Information and Other Associated Assets

i. Information assets shall only be used for legitimate business purposes in fulfilment of one’s roles and responsibilities to Stampede.

ii. All information created, sent, received or contained via Stampede IT Infrastructure are the property of Stampede and shall not be considered as private. It may be accessed and monitored by Stampede authorized personnel in accordance with the Stampede’s policies or governing laws and regulations.

iii. Retention period of the Stampede’s electronic data / information / documents that is stored in Stampede’s repository shall be determined by the respective business owners.

iv. Information shall be handled in accordance with Information Classification and Handling Procedure.

5.1.11 Return of Assets

i. Upon termination of employment or contract, all employees, contractors and third parties must return all Stampede owned and issued IT assets in their possession (including electronic and hardcopy documentation) to OPS or respective personnel.

5.1.12 Classification of Information

i. Information must be secured appropriately, in accordance with its security classification.

ii. Information must be appropriately classified in accordance with Stampede security classification as stated in Information Classification and Handling Policy.

5.1.13 Labelling of Information

i. Information must be appropriately labelled in accordance with Stampede security classification scheme as stated in Information Classification and Handling Policy.

5.1.14 Information Transfer

i. Transfer of classified information with Stampede and with any third party must be governed by contract or agreements.
ii. Transfer and sharing of Stampede information through collaborative technologies, social media or web mail must be carried out only once authorised in writing by the appropriate business and information owner. These must be controlled through Information Classification and Handling Policy.
iii. Transfer of information electronically and hardcopy must be protected against unauthorised access, misuse, or corruption in accordance with the handling requirements for the specific security classification of data contained on the media.
iv. Exposing Stampede applications' APIs to the general public and third parties must be controlled with adequate security controls as per the latest industry standards, commensurate with the associated risks.

5.1.15 Access Control

i. Access control lists and access mechanisms to control access between accounts and information must be established.
ii. Access control to information must be defined and documented by the asset owner(s) in accordance to the business requirements.

5.1.16 Identity Management

i. Unique identification for Stampede employees or any third parties that require access to Stampede assets must be used for detailed accountability of individual activity.
ii. User access management shall be implemented in accordance with Access Management Procedure.

5.1.17 Authentication Information

i. Password requirements must be adequately complex and strong, in accordance with the requirements specified in Access Management Procedure.
ii. Authentication information such as password and secret PIN must be stored centrally in a credential management system suitable to the technology domain where applicable.
iii. Authentication information must be stored in hashed and/or encrypted format using strong cryptography algorithms as per latest industry standards.
iv. Authentication information must be always encrypted during transmission over public networks.
v. Multifactor authentication must be implemented, wherever possible, for access to Stampede assets to achieve robust authentication method.

5.1.18 Access Rights

i. User must only be provisioned with the minimum permission required for them to perform their functions.
ii. User access management must be as per Stampede Access Management Procedure.
iii. Reviews of access must be performed at least annually in order to identify redundant user accounts and/or unnecessary privileges. When identified they must be disabled or removed from the system.
iv. The validity of access privileges must be confirmed periodically in accordance with the required business needs.

5.1.19 Information Security in Supplier Relationships

i. Stampede shall protect information assets that is accessible by suppliers.
ii. Project Owner shall ensure the information security requirements for mitigating the risks associated with supplier’s access to the information assets is agreed with the supplier and documented.
iii. Project Owner shall ensure arrangement involving suppliers shall be based on a formal Non-Disclosure Agreement (NDA).

5.1.20 Addressing Information Security within Supplier Agreements

i. All agreements including renewals of existing agreements with third parties must address information security requirements and include confidentiality or non-disclosure agreements.
ii. All agreements including renewals of existing agreements with third parties must provide Stampede with the right to audit security controls of the third parties to ensure that the controls implemented are sufficient to protect Stampede information assets in compliance with this policy.

iii. Compliance requirements must be defined in all new or renewed contractual agreements and regularly monitored.

5.1.21 Managing Information Security in the Information and Communication Technology (ICT) Supply Chain

i. Appropriate security controls and periodic monitoring must be in place to ensure that third party access to Stampede data is appropriately controlled and reviewed.

5.1.22 Monitoring, Review and Change Management of Supplier Services

i. The services, reports and records provided by third parties must be monitored and reviewed regularly (if needed).

5.1.23 Information Security for Use of Cloud Services

i. Stampede should maintain close contact with its cloud service providers.
ii. An agreement between the cloud service provider and Stampede, should include the following provisions for the protection of Stampede’s data and availability of services:

a. providing dedicated support, if necessary, in the event of an information security incident in the cloud service environment;

b. providing appropriate support and availability of services for an appropriate time frame when the Stampede wants to exit from the cloud service;

c. providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by Stampede, acting as the cloud service customer; and

d. providing and returning information such as configuration files, source code and data that are owned by Stampede, acting as the cloud service customer, when requested during the service provision or at termination of service.

5.1.24 Information Security Incident Management Planning and Preparation

i. Stampede Incident Management Procedure for managing information security incidents must be maintained to facilitate quick, effective, and orderly response in the event of a security incident.

ii. This must follow the Stampede Incident Management Procedure which includes, among others, clear roles and responsibilities, incident detection, analysis, containment, eradication, and recovery.

iii. Documentation must exist to ensure all employees and third parties are aware and use Stampede Incident Management Procedure in relation to security events, issues, and weaknesses.

5.1.25 Assessment and Decision on Information Security Events

i. All information security related events must be captured and analysed with key/critical events being reported to internal and external stakeholders (wherever applicable).

ii. Criteria for identifying and categorising information security events must be developed and implemented in accordance with Incident Management Procedure, and it must record evidence of an action associated with an event.

5.1.26 Response to Information Security Incidents

i. Incident response which includes containment, eradication and recovery phases must be executed based on the incident severity, impact, criticality of impacted asset and potential disruptions to business operations.

ii. External security and/or forensic experts may be used during the incident response should it deemed necessary.

5.1.27 Learning from Information Security Incidents

i. Post activity (i.e., post incident report, post-mortem meeting and improvement of incident response plan) must be defined and included in the Incident Management Procedure to reduce the likelihood or consequences of future incidents.

5.1.28 Collection of Evidence

i. Collection, acquisition, and preservation of evidence related to information security events must be included in the Incident Management Procedure to facilitate any disciplinary and legal actions.

ii. Where follow-up action against a person or organisation after a security incident involves legal action, evidence must be collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s) based on advice from Top Management.

5.1.29 Information Security During Disruption

i. Stampede Business Continuity Plan (BCP) must include requirements for information security and the continuity of information security management to ensure the continuity of critical business operations and the recovery of information assets in the event of disaster or disruption.

5.1.37 ICT Readiness for Business Continuity

i. Stampede BCP must include processes, procedures, and controls to ensure the required level of ICT continuity during an adverse situation.
ii. The processes, procedures and controls to ensure ICT continuity during an adverse situation must be tested at regular intervals in order to ensure that they are valid and effective.

5.1.38 Legal, Statutory, Regulatory, and Contractual Requirements

i. A formally documented list of all relevant legal and regulatory information security requirements must be maintained by ISMS Coordinator.

5.1.39 Intellectual Property Rights

i. Legislative, regulatory and contractual requirements on the use of proprietary software or materials subject to intellectual property rights must be adhered to in line with Stampede information security and other policies.

5.1.40 Protection of Records

i. Stampede records must be classified, stored, protected, and destroyed (after the retention period) in accordance with legal and business requirements. Information security logs must be maintained for a period approved by Top Management.
ii. The integrity of information on a publicly available system must be protected to prevent unauthorised modification.

5.1.41 Privacy and Protection of Personal Identifiable Information (PII)

i. Private or personal data collected in relation to individuals must be protected in line with Stampede Information Classification and Handling Procedure and applicable regulatory and contractual requirements.

5.1.42 Independent Review of Information Security

i. Stampede approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) must be reviewed independently at planned intervals, or when significant changes to the IT or security environment occur.

5.1.43 Compliance with Policies, Rules and Standards for Information Security

i. HoDs must ensure that information security procedures within their area of responsibility are carried out correctly to achieve compliance with Stampede Information Security Policy and associated security requirements.
ii. Technical compliance assessments must be regularly and independently performed to ensure that all IT systems have been implemented in a manner compliant with Stampede Information Security Policy and associated security requirements.
iii. In case of any conflict between this policy and any other policy in Stampede, the conflict must be brought to the notice of the CEO for his/her direction. In cases where no direction has been provided, this policy must take precedence.

5.1.44 Documented Operating Procedures

i. Operating procedures required to support the Stampede Information Security Policy must be documented, maintained, and made available to all users who need them.

5.2 People

5.2.1 Screening

i. Before hiring any candidate, an employment and qualifications reference check must be conducted.
ii. Private data collected in relation to individuals during the employment process must be protected in line with applicable privacy legislation relevant to the country of operation or as per relevant regulatory requirements.

5.2.2 Terms and Conditions of Employment

i. As part of their contractual obligation, employees, contractors and third-party users must agree and sign the terms and conditions of their employment contract, which must state their and Stampede responsibilities for information security.
ii. All employees, contractors and third parties who can access Stampede IT environment must comply with Stampede Information Security Policy and other applicable policies.

5.2.3 Information Security Awareness, Education and Training

i. An Information Security Awareness Program must be developed and maintained to educate and update all employees, contractors and third parties. The mandatory awareness trainings and activities must be performed at regular intervals.

5.2.4 Responsibilities After Termination or Change of Employment

i. The employment termination or change process must be managed by OPS.
ii. The Exit Process especially the return of all IT assets held must be strictly followed by the person (employee / contractor / third party user) leaving Stampede. This must be ensured by the person’s supervising manager along with OPS.
iii. All employees, contractors and third parties must have their access privileges to all Stampede IT tools revoked upon termination of their employment / contract.
iv. Changes of role must be reflected in the removal of all access privileges that were not approved for the new position.

5.2.5 Confidentiality or Non-Disclosure Agreements

i. Requirements for confidentiality or non-disclosure agreements reflecting Stampede needs for the protection of information must be identified and regularly reviewed.

5.2.6 Remote Working

i. Specific policies or procedures in compliance with Stampede Information Security Policy and operational plans must be developed and implemented for remote working activities. Remote working activities must be carried out in compliance with Stampede Company Policy.

5.2.7 Information Security Event Reporting

i. Employees or third-party users or service providers must report any security incidents or suspected security incidents to their immediate supervisor or through the dedicated reporting channel in Stampede.

5.3 Physical

5.3.1 Physical Security Parameters

i. All IT systems must be secured in locations that comply with Stampede's physical security requirements.

5.3.2 Physical Entry

i. Secure areas must be protected by appropriate physical entry controls to ensure that only authorised personnel are allowed access.
ii. Access points such as delivery and loading areas and other points where unauthorised persons may enter Stampede premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.
iii. Physical entry to Stampede Data Centre for Stampede employees as well as non-Stampede employees including vendors, contractors and external visitors must be recorded.

5.3.3 Securing Offices, Rooms and Facilities

i. All locations that house non-Data Centre computing facilities must be secured in line with the value, legal position, trust and sensitivity of the IT systems.

5.3.4 Physical Security Monitoring

i. Physical premises must be monitored by surveillance systems, which can include guards, intruder alarms, closed-circuit television (CCTV) and physical entry access system either managed internally or by a monitoring service provider.

5.3.5 Protecting Against Physical and Environmental Threats

i. Adequate physical protection against damages from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster must be designed and applied.

5.3.6 Working in Secure Areas

i. Physical protection and guidelines for working in secure areas must be designed and applied.

5.3.7 Clear Desk and Clear Screen

i. Inactive sessions must be configured to automatically terminate after 10 minutes.
ii. Appropriate compensating security controls, determined through a risk management process, must be implemented across IT systems that do not support session timeouts.
iii. Restrictions on connection times must be used to provide additional security for high-risk or critical IT systems or applications where appropriate.

5.3.8 Equipment Sitting and Protection

i. IT equipment must be located in physically secure and environmentally protected facilities, commensurate to the classification levels of the information held or processed.

5.3.9 Security of Assets Off-Premises

i. Appropriate security controls must be applied to off-site equipment, information and software, taking into account the different risks of working outside Stampede premises, if applicable.
ii. All mobile equipment approved to be taken off-site must be adequately protected and secured.

5.3.10 Storage Media

i. The management of removable media must be controlled.
ii. Media must be disposed of securely and safely when no longer required in accordance with the disposal requirements for the specific security classification of the data contained on the media.
iii. All media containing classified information must be stored securely according to Information Classification and Handling procedure.
iv. Media being transported must be protected from unauthorised access, misuse or corruption in accordance with the handling requirements.

5.3.11 Supporting Utilities

i. Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities by provision of suitable power backups.
ii. Supporting utilities must be regularly inspected and, as appropriate, tested to ensure their proper functioning and to reduce any risk from malfunction or failure.

5.3.12 Cabling Security

i. Power and telecommunications cabling carrying data or supporting information services must be protected from interception and damage. Protection must include physical access and technical controls commensurate to the sensitivity of the data the network carries.

5.3.13 Equipment Maintenance

i. Information processing facilities must be appropriately maintained to ensure its continued availability.

5.3.14 Secure Disposal or Re-use of Equipment

i. Prior to disposal or redeployment of storage media or devices, the data or information must be securely overwritten as per the industry standards to make the original information unrecoverable or reproducible.

5.4 Technological

5.4.1 User Endpoint Devices

i. Endpoint devices, issued to Stampede employees or third parties, and used outside Stampede facility, must not be left unattended and be physically secured, where possible, when left unattended.
ii. Where endpoint devices are in use or are left unattended, appropriate security controls must be implemented to mitigate risk associated with information theft, compromise and misuse.
iii. Endpoint devices, which process and/or store classified information must have a power on password and appropriate encryption implemented.
iv. Users must appropriately secure unattended equipment by terminating active sessions when finished or by activating an appropriate locking mechanism (such as locking the computer).

5.4.2 Privileged Access Rights

i. The privileged access rights must be restricted and managed, wherever possible, with a privileged access management tool, in accordance with Stampede Access Management Procedure.

5.4.3 Information Access Restriction

i. Access to IT applications and systems must be restricted in accordance with business needs and Stampede Access Management Procedure.

5.4.4 Access to Source Code

i. Access to program source code, if stored on Stampede IT systems, is restricted and on need-to-know basis. Access to program source code must only be provided based on written request. This access must be time based and must be terminated once the approved time has expired.
ii. Strict security control must be maintained over access to program source code as per access control and information access restriction requirements of this policy.

5.4.5 Secure Authentication

i. Access to system level functions across all information systems must be controlled using appropriate secure log-on process and controls.
ii. Access to operating systems must be controlled by a secure log-on procedure.

iii. Identities must be authenticated before accessing trusted services. For critical services or services identified with high risk, identities must be authenticated with at least two factor authentication method.

5.4.6 Capacity Management

i. Respective departments are responsible for monitoring the capacity utilisation with alerts raised to the System/Application Owners once the systems reach 80% capacity utilisation. System/Application Owners are responsible to plan for capacity management of all IT systems to ensure their continuous availability.

5.4.7 Protection Against Malware

i. Controls must be implemented to prevent, detect, respond and recover from malicious software (malware) or tools.
ii. Users must be prohibited from disabling or reconfiguring malware protection software or systems.
iii. User awareness training on cyber threats and malicious software must be performed on a regular basis.
iv. Malware signatures or any other behavioural patterns must be regularly updated, kept current and maintained.
v. Only Stampede approved and authorised software or tools must be used in Stampede IT systems and environment.
vi. Where the use of mobile code is authorised, the configuration must ensure that the authorised mobile code operates securely, and that unauthorised mobile code must be prevented from being executed.

5.4.8 Management of Technical Vulnerabilities

i. Management of technical vulnerabilities must be carried out as per relevant guidelines.
ii. It is mandatory to report to the relevant personnel if any IT security vulnerabilities observed by employees and/or vendors and/or business partners.
iii. Any Stampede appointed third party service provider are NOT allowed to run exploits on IT systems, networks, applications and users whether belonging to Stampede or any other organisation or individual.
iv. Stampede approved IT systems hardening standards must be applied on all IT systems where applicable. Hardening standards are to be approved by the Top Management.
v. All Stampede personal computers including laptops and workstations must be built on a standard configuration (image) as per the industry standard.

5.4.9 Configuration Management

i. Configuration standards must be created/adopted for all critical IT systems (including hardware, network devices and software). All IT systems must be configured in compliance with Stampede approved standards.
ii. All default or vendor-supplied settings must be reviewed and changed where necessary before installing a system on the network (this includes passwords, remote management functionality and generic accounts).

5.4.10 Information Deletion

i. Information stored in information systems, devices or in any other storage media should be deleted when no longer required and when applicable.
ii. When deleting information on systems, applications and services, the following should be considered:
   a. The results of deletion are recorded as evidence;
   b. When using service suppliers of information deletion, evidence of information deletion from them is obtained.

iii. The types of information that should be deleted when no longer required are:
   a. Personal Data: This includes any information that can be used to identify an individual, such as names, addresses, social security numbers, and personal health information. Secure deletion is critical to comply with data protection regulations like PDPA which mandate the protection of personal data.
   b. Confidential Business Information: Proprietary data such as trade secrets, confidential corporate strategies, internal reports, and financial information should be securely deleted to prevent unauthorized access that could harm the business.
   c. Financial Information: This includes bank account details, credit card numbers, transaction records, and other financial data that, if accessed by unauthorized parties, could lead to financial fraud or identity theft.
   d. Employment Details: Information about employees, including performance reviews, employment history, and other personal employee data, should be securely deleted when no longer needed to protect privacy and comply with employment laws.
   e. Customer Data: Stampede often collect customer information for business purposes. This data should be securely deleted once it is no longer necessary to protect customer privacy.

f. Old Electronic Correspondence: Emails, messages, and other digital communications that contain sensitive information should be securely deleted to ensure that remnants of data do not pose a security risk.

iv. Methods of deleting sensitive information include, but are not limited to:

a. Configuring systems to securely destroy information when no longer required (e.g., after a defined period subject to the topic-specific policy on data retention or by subject access request);

b. Deleting obsolete versions, copies and temporary files wherever they are located;

c. Using approved, secure deletion software to permanently delete information to help ensure information cannot be recovered by using specialist recovery or forensic tools; or

d. Using disposal mechanisms appropriate for the type of storage media being disposed of (e.g., degaussing hard disk drives and other magnetic storage media)

5.4.11 Data Masking

i. Where the protection of sensitive data (e.g., PII) is a concern, Stampede must consider hiding such data by using techniques such as data masking. The version with the masked information can then be used for various purposes, such as user training or software testing.

ii. Techniques for data masking include, but are not limited to:

a. Encryption (requiring authorised users to have a key);
b. Nulling or deleting characters (preventing unauthorised users from seeing full messages);
c. Varying numbers and dates;
d. Substitution (changing one value for another to hide sensitive data); or
e. Replacing values with their hash.

5.4.12 Data Leakage Prevention

i. Data leakage prevention measures must be applied to systems, networks and any other devices that process, store or transmit sensitive information to detect and prevent the unauthorised disclosure and extraction of information by individuals or systems.

ii. The following controls should be considered to reduce the risk of data leakage:

   a. Identifying and classifying information to protect against leakage (e.g., personal information, product designs, etc);

   b. Monitoring channels of data leakage (e.g., email, file transfers, mobile devices, and portable storage devices); or

   c. Acting to prevent information from leaking (e.g., quarantine emails containing sensitive information, blocking USB port at endpoint devices, and mobile application management).

5.4.13 Information Backup

i. Stampede shall conduct backup to protect against loss of data.

ii. Backup shall be performed in accordance with the third-party service provider terms of service, if applicable.

iii. Adequate backup facilities must be in place to ensure all Stampede critical IT Infrastructure and application systems can be recovered following a disaster or hardware/software failure.

5.4.14 Redundancy of Information Processing Facilities

i. Information processing facilities at Stampede must be implemented with redundancy sufficient to meet availability requirements to ensure the continuous operation of information processing facilities.

ii. Same security level as the primary ones should be ensured at the redundant components and information processing facilities.

iii. Redundant information processing facilities must be tested on periodic basis to ensure the failover from one component to another component works as intended.

5.4.15 Logging

i. Audit logging features shall be enabled to capture changes to sensitive information in all production application systems that track every addition, modification and deletion of information.
ii. All information security event logs shall be reviewed periodically.
iii. Logs pertaining to confidential and critical assets must be retained in compliance with regulatory and internal business requirements.
iv. Logs must be monitored, and an appropriate response process activated when undesirable security events are detected.
v. Processes must be in place to actively log, manage and response to system faults or abnormal activities.

5.4.16 Monitoring Activities

i. The following periodic activities must be put in place as part of the monitoring mechanism:

   a. Vulnerability assessment and penetration testing must be done periodically.
   b. Security monitoring and event detection must be put in place and the effectiveness of the security monitoring and event detection must be reviewed periodically.

5.4.17 Clock Synchronisation

i. All IT system clocks must be synchronised to Stampede approved centralised time server.

5.4.18 Use of Privileged Utility Programs

i. The use of utility programs that might be capable of overriding system and application controls, such as vulnerability assessment and/or penetration testing applications must be restricted and tightly controlled.

5.4.19 Installation of Software on Operational Systems

i. Only genuine software is permitted to be installed on Stampede-related end devices.

5.4.20 Networks Security

i. The security gateway between network zones must:

   a. Provide filtering and packet analysis on the information which passes between the logical networks.
   b. Be used as a means of controlling access to and from Stampede network.

ii. External connection to Stampede IT system must be through approved remote access solutions.

iii. An approved secure authentication control must be implemented for all users accessing the corporate network and services from remote locations over untrusted networks.

iv. Wireless Networks:

   a. Access to wireless network must be protected in accordance with Stampede business requirements.
   b. Wireless access points must be installed based on request raised by the department requesting and approved by Top Management.
   c. All wireless devices must have at least WPA2 encryption and set with strong password.

5.4.21 Security of Network Services

i. A list of standard services that are permitted on the internal network must be formally maintained.

ii. Security features, service levels and management requirements, for services being provided by an internal or third party must be included in all service agreements.

5.4.22 Segregation of Networks

i. Network must be segregated based on assessed risks into different logical network zones with suitable security gateway arrangements. De-militarised zones must be established between all untrusted networks (such as the Internet or Public networks) and information systems storing classified information. Network segments should be properly configured with sub-netted IP addresses, eliminating the existence of flat network architecture.

ii. Appropriate logical and physical network segregation techniques must be used to restrict traffic flow based on business requirements, risk assessment, data sensitivity and asset critically.

5.4.23 Web Filtering

i. The risk of employee accessing websites that contain illegal information or are known to contain viruses or phishing material must be reduced through techniques such as blocking the IP address, or the domain of the website(s) concerned.
ii. Blocking of the following types of websites must be considered:
    a. Known or suspected malicious websites (e.g., those distributing malware or phishing contents);
    b. Command and control servers;
    c. Malicious website acquired from threat intelligence;
    d. Websites sharing illegal content.

5.4.24 Use of Cryptography

i. A standard on the use of cryptographic controls for the protection of information assets must be used in compliance with all relevant agreements, laws, and regulations.
ii. All critical business applications that collect, transmit, process or store classified data must make use of secure authentication methods and implement appropriate cryptographic controls.
iii. Digital certificates must be used by Stampede to secure all network communication, including email, web traffic and file transfers.
iv. All digital certificates used by Stampede must be issued by a trusted Certificate Authority (CA).
v. All cryptographic keys must be protected against deliberate or accidental misuse, modification and destruction by adopting suitable key management requirements.

5.4.25 Secure Development Life Cycle

i. Rules for secure development of software and system must be established and applied to ensure information security is designed and implemented within the secure development life cycle as per Stampede System Development Procedure.

5.4.26 Application Security Requirements

i. Information security requirements must be identified, specified, and approved when developing or acquiring applications as per Stampede System Development Procedure.

5.4.27 Secure System Architecture and Engineering Principles

i. Security engineering principles must be established, documented, and applied to information system development activities as per Stampede System Development Procedure.
ii. System documentation must be protected from unauthorised access and modification in accordance with its security classification.

5.4.28 Secure Coding

i. Process/Principles to provide good governance for secure coding must be applied during software development to ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.
ii. The following best practices for secure coding must be considered:
   a. Code minification and obfuscation;
   b. Avoiding shortcuts;
   c. Automated scanning and code reviews;
   d. Avoiding components with known vulnerabilities;
   e. Avoiding hardcoded access keys;
   f. Auditing and Logging.

5.4.29 Security Testing in Development and Acceptance

i. Formal testing and acceptance criteria must be implemented for all new or upgraded critical IT systems. Testing must be carried out prior to acceptance.
ii. Where practical, operating systems, software, firmware and updates must be tested prior to deployment. Each patch must be reviewed for potential impacts and tested prior to inclusion in the production environment.

5.4.30 Outsourced Development

i. Where system development is outsourced, the requirement and expectation must be communicated and agreed by Stampede. The delivery of outsourced services must be continually monitored and reviewed to ensure it meets the expectations.

5.4.31 Separation of Development, Test, and Production Environments

i. Development and testing environments must be separated from the operational environments. Rules for the migration of systems from development to operational status must be defined and documented.
ii. Where a fault cannot be replicated in a testing environment, production testing and resolution must follow documented change control procedures.

5.4.32 Change Management

i. Changes to information processing facilities and systems must be controlled according to the Stampede Change Management Procedure.
ii. Before approval, changes to critical systems must be tested in a separate environment from production, where available, to prevent unforeseen impacts on production data and systems.

5.4.33 Test Information

i. All business units must maintain test data which is similar to production data but not from production. Production data must not be used for testing unless authorised in writing by the data owner.
ii. Where production data is used in pre-production or testing environments, appropriate approvals must be obtained for the individuals accessing the data.
iii. The level of security protection for test data must be determined through a risk management process.

5.4.34 Protection of Information Systems During Audit Testing

i. Planning and scheduling audit requirements must be performed in conjunction with information asset owners to minimise the risk of disruptions to business processes.

6.0 APPENDIX

Not applicable.