Revision	Prepared by	Date
Version 1	Commercial Team	09/03/2020

SECURITY AND CRISIS PROTECTION POLICY

DISCLAIMER

This “Security & Crisis Protected Policy (SCPP)” is embodiment of execution plan, guideline, or references to initiate, establish and support or mitigate the situation in related to information technology or technology stack paradigm, cloud technology, network security, IT product and IT practice.

All related policy has its own extension according to the following section:-

Information Logging Standard	Defines the specific requirements for information systems to generate appropriate audit logs that will integrate with an enterprise's log management function.	22
Cloud Instance/Server Security Policy	Defines standards for minimal security configuration for servers inside the cloud application production, or used in a production capacity.	26
Software Installation Policy	Defines the requirements around installation of third party software on company cloud services	29
Application		
Web Application Security Policy	Defines the requirement for completing a web application security assessment and guidelines for completing the assessment.	31
Old/Retired		
Server Audit Policy	Defines baseline configuration standards for servers installed on the company network. Relevant content was added to the new Workstation Configuration Standard.	

General Section
Acceptable Encryption Policy

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the Malaysia and World Wide Web.

3. Scope

This policy applies to all ODELA employees and affiliates.

4. Policy

4.1. Algorithm Requirements

4.1.1. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

4.1.2. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

4.1.3. Signature Algorithms

Algorithm	Key Length /Description	Additional Remark
RSA	2048bit	N/A
SHA	256	N/A
SSL	Digital Validation	Domain
TLS 1.2	• Ed25519 , ed448 signature added. • Exchange at x25519 and x448 key exchange. • DH-RSA enabled. • DHE-RSA enabled.	Define by RFC 5246. Supported and well protect from MITM

	• ECDHE-RSA enabled. • DH-DSS enabled. • PSK and PSK-RSA enabled. • DHE-PSK • ECDHE-PSK enabled. • SRP enabled. • SRP-DSS enabled. • SRP-RSA enabled.	

4.2. Signature Algorithms

In general, the company adheres to the NIST Policy on Hash Functions.

4.2.1. Key Agreement and Authentication

4.2.1.1. Key exchanges must use one of the following cryptographic protocols: Diffie- Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

4.2.1.2. End points must be authenticated prior to the exchange or derivation of session keys.

4.2.1.3. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

4.2.1.4. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

4.2.1.5. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.3. Key Generation

4.3.1. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.3.2. Key generation must be seeded from an industry standard random number generator (RNG). By following NIST standard (https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexc.pdf)

5. Compliance

5.2. Compliance Measurement

The Tech team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.3. Exception

Any exception to the policy must be approved by Tech Team in advance.

5.4. Non-Compliance

Any user, merchant, sellers or 3rd party engagement whom found to have violated this policy may be subject to disciplinary action, up to and including termination of contract, and impose penalty or court.

6. Related Standard

Code Title	Link
National Institute of Standards and Technology (NIST) publication FIPS 140-2	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
NIST Policy on Hash Function	

7. Definition of term

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

7.2. Proprietary Encryption

8. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

General Section
Acceptable Use Policy

1. Overview

Tech Team's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the company established culture of openness, trust and integrity. Tech Team is committed in protecting company product, application, and infrastructure from illegal or misuse or damaging actions by individuals, either knowingly or unknowingly.

The communication could be or either from Internet/Intranet/Extranet-related systems, including but not limited to any IT product, application and infrastructure. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems and applications.

2. Purpose

The purpose of this policy is to outline the acceptable use of IT product and application. These rules are in place to protect the employee and the company. Inappropriate use exposes the company to risks including virus attacks, malware, compromise of network systems/ cloud and services, and legal issue.

3. Scope

This policy applies to the use of information, electronic and computing devices, network resources and cloud computing to conduct business or interact with internal networks and business systems, the employee, or a third party.

All employees, contractors, consultants, temporary, and other workers at the company and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the company policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

4. Policy

4.1. General Use and Ownership

4.1.1. The company proprietary information stored on Cloud.

4.1.2. All technical proprietary information is stored in cloud repository (gitlab).

4.1.3. Every fortnightly, there will be a housekeeping and at the same time done to report any if it has any closure. Promptly report when there is a theft, loss or unauthorized disclosure of the company proprietary information.

4.1.4. Currently, proprietary information only to the extent it is authorized and necessary to fulfil certain assigned member depending on job duties.

4.1.5. Employees are responsible for exercising good judgment regarding the reasonableness of working use.

4.1.6. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult with CTO.

4.1.7. For security and network maintenance purposes, authorized individuals within the company may monitor application, cloud instances, systems and network traffic at any time, per Tech Team's *Audit Policy*.

4.1.8. The company reserves the right to audit networks, cloud and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary information

4.2.1. All mobile and computing devices that connect to the internal network must comply with the ***minimum security step policy***.

4.2.2. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3. All computing devices must be secured with a password-protected and exit from terminal or cloud console either with screensaver or with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4. Postings by employees from the company by using company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of with the company, unless posting is in the course of business duties.

4.2.5. Employees must use extremely cautios when opening e-mail attachments, received feedback from support ticketing system. All received from unknown senders or non-verified, may contain malware.

4.3. Unacceptable Use

The following activities are in general prohibited. Employee may be exempted from these restriction during the course of their legitimate job responsibilities. In example, System administration staff may have a need to disable network connection to instances if that host is disrupting production services.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.3.1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, Forging repository.

4.3.1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which company or the end user does not have an active license is strictly prohibited.

4.3.1.3 Accessing data, a server or an account for any purpose other than conducting company (or in IT product or Odela) business, even if you have authorized access, is prohibited. Unless, with the permission from CTO.

4.3.1.4 Exporting software, database information (refer to Database Credentials Policy), technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.1.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.3.1.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.1.7 Using the company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.3.1.8 Making fraudulent offers of products, items, or services originating from any company product, company cloud instances account.

4.3.1.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.3.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.3.1.11 Port scanning or security scanning is expressly prohibited unless prior notification to tech team is made.

4.3.1.12 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

4.3.1.13 Circumventing user authentication or security of any host, network or account.

4.3.1.14 Introducing honeypots, honeynets, or similar technology on the company cloud network.

4.3.1.15 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.3.1.16 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.17 Providing information about, or lists of, company employees to parties outside or vice versa with data of registration program.

5. Compliance

5.1. Compliance Measurement

The Tech Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

6.1. Data Classification Policy

6.2. Data Protection Standard

6.3. Minimum Access Policy

6.4. Password Policy

6.5. Minimum Security Step Policy (MSSP)

7. Definitions and Terms

7.1. Honeypot

7.2. Honeynet

7.3. Proprietary Information

8. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

General Section
Password Construction Policy

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

2. Purpose

The purpose of this guidelines is to provide best practices for the created of strong passwords.

3. Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

4. Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. The system, application, cloud console recommend a minimum of 8 characters in your password. In addition, we highly encourage the use of passphrases, passwords that are made up of multiple words, numbers, and symbol that mix up. Examples include "*P@$$W0rd*" or "*/\/\@L@ys1a*". Passphrases are both easy to remember and type, yet meet the strength requirements. Check the following password guideline creation:

4.1. Contain eight characters or more.

4.2. Does not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

4.3. Avoid password patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

4.4. Avoid some version of password like "Welcome123", "Password123" and "Changeme123".

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

5. Policy

5.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

General Section
Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of company resources. All staff, including contractors and vendors with access to company Cloud console or product systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system.

This include :

- Application / Session
- Cloud Console
- Cloud Instances
- Repositories

4. Policy

4.1. Password Creation

4.1.1. All user-level and system-level passwords must conform and refer to the *Password Construction Guidelines*.

4.1.2. Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.3. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

4.2. Password Change

4.2.1. Passwords should be changed only every 3 month or 90 days and also when there is reason to believe a password has been compromised.

4.2.2. Password cracking or guessing may be performed on a periodic or random basis by the Tech Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3. Password Protection

4.3.1. Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, Confidential information.

4.3.2. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3. Passwords may be stored only in “password managers” authorized by the organization or approved password Manager tools.

4.3.4. Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5. Any user suspecting password may have been compromised must report the incident directly to Tech Team and change all passwords.

4.4. Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1. Applications must support authentication of individual users, not groups.

4.4.2. Applications must not store passwords in clear text/plain-text or in any easily reversible form.

4.4.3. Applications must not transmit passwords in clear text over the network.

4.4.4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

In condition of:

- Through IAM for cloud console.
- Role user that has features enable.

4.5. Multi-Factor Authentication

4.5.1. Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.
- At Cloud console.

5. Policy Compliance

5.1. Compliance Measurement

The Tech Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, data/screen monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Tech Team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

6.1. Password Construction Guidelines

7. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

General Section
Security Response Plan Policy

1. Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

2. Purpose

The purpose of this policy is to establish the requirement that all business units supported by the Tech Team develop and maintain a security response plan. This ensures that security incident management has all the necessary information to formulate a successful response should a specific security incident occur.

3. Scope

This policy applies any established and defined business unity or entity within the company. This include any application, or IT product in the company.

4. Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation and maintained by the Tech Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit coordinator is further expected to work with the Tech Team in the development and maintenance of a Security Response Plan.

4.1. Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2. Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3. Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4. Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5. Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5. Compliance

5.1. Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2. Exception

Any exception to this policy must be approved by the Tech Team in advance and have a written record.

5.3. Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP.

6. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Cloud Security
Database Credentials Policy

1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one or more company IT product and applications.

External software applications running on company networks may require access to one of the many database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding the applications that will access a production and staging database server on the company cloud instances. This policy applies to all software (programs, modules, libraries or API that will access the application or system, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments. Always sanitized the code before push to the instances. Most application and system databases are stored in cloud.

4. Policy

4.1. General

In order to maintain the security of cloud databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server. All credential connectivity must assigned to cloud IAM and security group, in order to avoid any anomalies.

4.2. Specific Requirements

4.2.1. Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the Password Policy.

4.2.2. Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

4.2.3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

- Database passwords used by programs are system-level passwords as defined by the Password Policy.

- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

5. Compliance

5.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the company.

Any program code or application that is found to violate this policy must be remediated within a 90 day period.

6. Related Standard, Policies and Processes

- Password Policy.

7. Definitions and Terms

- Credentials
- Executing Body
- Hash Function
- Module

8. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Cloud Security
Technology Equipment Disposal Policy

1. Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both responsible and often required by law.

In normal traditional everything will be involve with hardware like hard drives, USB drives, CD-ROMs and other storage media contain various kinds of company data, but, nowadays everything is at cloud services. In order to protect our constituent's data, all cloud service, especially storage mediums must be properly erased before being destroy its instances.

When deleting files or formatting a data, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to instance disposal.

2. Purpose

The purpose of this policy it to define the guidelines for the disposal of technology and components owned/subscribe by the company.

3. Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within the company including cloud storage/instances.

All company employees and affiliates must comply with this policy.

4. Policy

4.1. Technology Equipment Disposal

When Technology assets have reached the end of their useful life they should be backup for law purposes.

4.1.1. The Tech Teams will securely erase instances, or any mediums in accordance with current industry best practices.

4.1.2. All data including, all files and licensed software shall be removed adequately in proper manner. Each activity must be recorded.

4.1.3 No cloud instance or technology that subscribe sold to any individual other than through the processes identified in this policy (Section 4.2 below).

4.1.4. Reinitialize disk or Reflash instances may need to consult to CTO in each of its activity.

4..5. Any overwritten application, or server setting that impact commercially may need approvable for its changes or deletion of module dependencies.

4.1.6. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed. However, it must be recorded and approved by CTO.

- Employee/Subsidiary Purchase of Disposed Instances and resources.

4.2.1. All instances that which is working, does not have end of life. Therefore, doesn't entitle for available purchasing.

4.2.2. Finance and Tech Team will determine an appropriate cost for each item if any potential partner or collaboration need resources (eg. instances, databases, firewall and etc).

4.2.3. Refer to commercial term and condition.

4.2.4. Prior to leaving the company (subject to staff termination or resignation), all jotted structure and cloud console setup and details must be update to latest definition at masterlist.

5. Compliance

5.1. Compliance Measurement

The Tech Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Tech Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Cloud Security
Information Logging Standard

1. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

2. Purpose

The purpose of this documenting attempts is to address the issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3. Scope

This policy applies to all production systems on all subscribe cloud services.

4. Policy

4.1. General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What the activity was performed on (object)?
- When was the activity performed?

- What tool(s) was the activity was performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

4.2. Activities to be logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords.
- Create, update, or delete information not covered in #1.
- Initiate a network connection.
- Accept a network connection.
- User authentication and authorization for activities covered in #1 or #2 such as user login and logout.
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes.
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes.
- Application process startup, shutdown, or restart.
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault.
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3. Elements of logged

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete, and accept

- network connection.

- Subsystem performing the action – examples include process or transaction name, process or transaction identifier.

- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

- Before and after values when action involves updating a data element, if feasible.

- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.

- Whether the action was allowed or denied by access-control mechanisms.

- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4. Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

- Operating System Event Logs collected by a centralized log management system.

- Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system.

- Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document.

- Other open logging mechanisms supporting the above requirements including those based on Graylog, ELK (Logs), Syslog, CheckPoint OpSec, ArcSight CEF, and IDMEF.

5. Compliance

5.1 Compliance Measurement

The Tech team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Tech team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Cloud Security
Cloud Instance/Server Security Policy

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2. Purpose

The purpose of this policy is to establish standards for the base configuration of cloud services that is owned and/or operated by the company. Effective implementation of this policy will minimize unauthorized access to the company proprietary information and technology, and cloud services.

3. Scope

All employees, contractors, consultants, temporary and other workers at the company and its subsidiaries must adhere to this policy. This policy applies to cloud resources that is operated, or subscribe by the company or registered under an internal network domain.

4. Policy

4.1. General Requirement

4.1.1. All cloud services deployed by the company subscribe is supervision by an operational group. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Tech team. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Tech team.

The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact.

- Server contact(s) and location, and a backup contact.
- Hardware and Operating System/Version.
- Main functions and applications, if applicable.
    - Information in the corporate enterprise management system must be kept up-to-date.
    - Configuration changes for production servers must follow the appropriate change management procedures.

4.1.2. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit Policy.

4.2. Configuration Requirement

4.2.1. Operating System configuration should be in accordance with approved Tech team guidelines.

4.2.2. Services and applications that will not be used must be disabled where practical.

4.2.3. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

4.2.5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

4.2.6. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

4.2.7. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

4.2.8. Servers should be access-controlled environment.

4.3. Monitoring

4.3.1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2. Security-related events will be reported to Tech team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security related events include, but are not limited to:

- Port-scan attacks.
- Evidence of unauthorized access to privileged accounts.
- Anomalous occurrences that are not related to specific applications on the host.

5. Compliance

5.1. Compliance Measurement

The Tech team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Tech team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standard, Policies and Processes

- Audit policy

7. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Cloud Security
Software Installation Policy

1. Overview

Allowing employees to install software on company cloud computing services opens the organization up to unnecessary exposure. Conflicting file versions or resources or dependencies which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company cloud services.

2. Purpose

The purpose of this policy is to outline the requirements around installation software on company cloud services. To minimize the risk of loss of program functionality, the exposure of sensitive information contained, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This policy applies to all company employees, contractors, vendors and agents with a cloud instance/services. This policy covers all computers, servers, smartphones, tablets and other computing devices that access the cloud console and instances.

4. Policy

4.1. Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email.

4.2. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.

4.3. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

5. Compliance

5.1. Compliance Measurement

The Tech team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Application
Web Application Security Policy

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within company application and services. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of company product services that available in public as well as satisfy compliance with any relevant policies in place or for collaboration.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at company cloud services. All web application security assessments will be performed by delegated security personnel either employed or contracted by the company. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of company is strictly prohibited unless approved by the CTO.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1. Web applications are subject to security assessments based on the following criteria:

- New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

- Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

- Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

- Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such CTO or an appropriate manager who has been delegated this authority.

4.2. All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

- Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

- Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3. The following security assessment levels shall be established by the tech team of organization or other designated organization that will be performing the assessments.

- Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use

manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

- Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

- Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4. The current approved web application security assessment tools in use which will be used for testing are:

- gitlab Unit Testing
- php spec
- selenium
- specflow
- scripting
- gremlin

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

5. Compliance

5.1. Compliance Measurement

The Tech team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Tech team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6. Related Standard, Policies and Processes

- OWASP Top Ten Project
- OWASP Testing Guide

- OWASP Risk Rating Methodology

7. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A

Old/Retired
Server Audit Policy

1. Overview

See purpose.

2. Purpose

The purpose of this policy is to ensure all servers deployed at cloud services that are configured according to the company security policies. Servers deployed at subscribe cloud console shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:
- Ensure integrity, confidentiality and availability of information and resources.
- Ensure conformance to company cloud security policies.

3. Scope

This policy covers all servers company subscribe or operated by company. This policy also covers any server/instances present on cloud console, but which may not be owned or operated by company.

4. Policy

The company hereby provides its consent to allow auditor to access cloud services to the extent necessary to allow audit to perform base on scheduled and ad hoc audits of all cloud services servers at company cloud console.

4.1. Specific Concerns

Servers in use for company support critical business functions and store company
sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of these systems.

4.2. Guideline

Approved and standard configuration templates shall be used when deploying server systems to include:

- All system logs shall be sent to a central log review system.
- All Sudo / Administrator actions must be logged.
- Use a central patch deployment system.
- Host security agent such as antivirus shall be installed and updated.
- Network scan to verify only required network ports and network shares are in use.
- Verify administrative group membership at Cloud IAM.
- Conduct baselines when systems are deployed and upon significant system changes .
- Changes to configuration template shall be coordinated with approval of change control board.

4.3. Responsibility

auditor shall conduct audits of all servers owned or operated by company. Server and application owners are encouraged to also perform this work as needed.

4.4. Relevant Findings

All relevant findings discovered as a result of the audit shall be listed in the company tracking system to ensure prompt resolution or appropriate mitigating controls.

4.5. Ownership of Audit Report

All results and findings generated by the audit Team must be provided to appropriate company management within one week of project completion. This report will become the property of company and be considered company confidential.

5. Compliance

5.1. Compliance Measurement

Auditor shall never use access required to perform server audits for

any other purpose. Tech Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Tech Team in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date Change	Carried Out	Summary Changes	Remark
6/03/2020	Tech Team: Ts. Muhammad Johar Jaafar	Initial Roll-out	N/A