YINSON HOLDINGS BERHAD

Information Security

POLICY & PROCEDURE

01	12-Jun-2020	Issue for Approval	Legal Counsel	Head of IT	Board
Rev No.	Date	Reason for Issue	Prepared by	Checked by	Approved by

Document Title:	Information Security Policy & Procedure		
Document No:	YHB-IT-CG-PP-0001		
Process:	IT & Technology	**Applicable To:**	YINSON Group of Companies
Revision No:	01	**Effective Date:**	12 June 2020

Table of Contents

Revision Details

Rev. No.	Section	Details
01		New Policy Adoption

OBJECTIVE:

We view it as our duty, as an international corporation, to comply with the various legal regulations around the world that govern the management of generating, storage and exchange of information data. Our top priority is to ensure universally applicable, worldwide standards for handling information data within our Group.

For us, protecting the personal rights and privileges of each and every data subject is the foundation of trust in our business relationships.

We shall achieve this by:

We are at an era which is often referred to as the "information age". There have been massive changes in the way humans generate, store and exchange information. We have accrued great benefits from this new era, but it brings with its profound challenges in the areas of security and privacy, which have been reflected in the growth of legislation around the globe concerning the holding of information. We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure; is accurate, timely and attributable; and is available to those who should be able to access it. The Information Security Policy below provides the framework by which we take account of these principles. This Information Security Policy ("The Policy") goes hand in hand with Yinson Group of Companies' ("Yinson's Group") Data Privacy Policy. So, what is the link between Information Security Policy and Data Privacy Policy? A well-designed and executed information security policy ensures both data security and data privacy. An information security policy is simply the means to the desired end, which is data privacy. Its primary purpose is to enable all of Yinson Group's employees to understand both their legal and ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways. This policy is the cornerstone of Yinson Group's on-going commitment to enhance and clarify our information security procedures.

This policy is applicable to all Yinson Group personnel, contractors and visitors engaged in activities under the Yinson Group.

The Group Chief Executive Officer of Yinson Holdings Berhad is accountable to the Board of Directors for ensuring that this policy is implemented in its entirety.

This policy will be reviewed every two years or as required.

1 CHAPTER I: OBJECTIVES AND DEFINITION

1.1 Objective & Scope

a) This Policy shall establish a framework for the responsible management of information security.

b) This policy applies to all Yinson Employees; as well as vendors, contractors, partners, collaborators and any others doing business with Yinson Group will be subject to the provisions of this Policy. Any other parties, who use, work on, or provide services involving Yinson Group's computers and technology systems will also be subject to the provisions of this Policy. Every user of Yinson Group's computer/IT resource is expected to know and follow this Policy.

c) Under the terms of their contract with Yinson group of companies ("Yinson Group"), all Yinson Employees who have been authorised access to Yinson's confidential information are responsible for handling such information and maintaining confidentiality appropriately at all times. This policy may be subject to change and be amended at any time.

d) Any breach of this policy will be taken very seriously and employees who act outside the requirements or guidance set out in this policy will be asked to explain the reasons for their actions and may face disciplinary action. Wilful and negligent non-adherence to this policy by any employee is a serious disciplinary matter which may result in dismissal.

e) All Yinson Employees and authorized third parties are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

1.2 Ownership

This standard and its sub-documents belong to the **Head of IT Department** (or his delegate) and shall not be altered without signed Approval.

The procedure is applicable for all Yinson Group’s managed documents.

1.3 Abbreviations & Definitions

The Definitions below are the Yinson Group’s standard for all managed documents.

YHB	Yinson Holdings Berhad
“**Yinson Employee**”	includes permanent worker, temporary worker, trainees of the Yinson Group;

2 CHAPTER II: APPLICATION OF NATIONAL LAWS

2.1 Application of National Laws

This Policy does not replace the existing national laws and instead supplements the various information security related laws, if any. The relevant national law will take precedence in the event that it conflicts with this Policy, or it has stricter requirements than this Policy.

The respective Yinson department head/managers are responsible for ensuring the relevant department's compliance with this Policy.

3 CHAPTER III: INFORMATION SECURITY TEAM STRUCTURE

3.1 Yinson Group Information Security Team Structure

The Information Security Team for each office includes:

- Yinson Group's Information Technology Department designated for the respective office;
- the Data Privacy Officers designated for the respective office.
- The Human Resources Department designated for the respective office.
- The Administration Department designated for the respective office.

The Head of Information Technology Department and the Chief Data Privacy Officer together with the relevant Yinson office's Human Resource Department Head and Administration Department Head shall be overseeing this initiative.

NOTICE: SUB POLICIES

Yinson Information Security Policy comprises of other sub-policies, including, but not limited to, the IT Security Policy and Remote Access Policy, that address specific areas of information security. Yinson Group departments may also have internal policies relevant to the subject matter associated with the specific work of the department. In the event of a conflict, the policies providing the Yinson Group with the greatest level of security will be applied, which shall be determined by the Information Security Team.

4 CHAPTER IV: POLICIES

4.1 Information Classification Policy

4.1.1 All data at Yinson Group shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with the aggregated information.

a) Restricted: Data in any format collected, developed, maintained or managed by or on behalf of Yinson Group, or within the scope of Yinson Group's activities. These data are highly confidential and only restricted to certain departments or personnel within Yinson, which, if exposed or breached, could result in a high amount of legal damages, fines/penalties, identify theft and/or financial fraud. (Examples include pricing information in relation to project bids. Such information may be only privy to certain Yinson Employees of a certain position or department).

b) Confidential: Data whose loss or unauthorized disclosure would impair the functions of Yinson Group, cause significant financial or reputational loss or lead to likely legal liability, though not as high as that of Restricted Data. (Examples include documents received from third parties which was received through confidentiality agreements/NDAs. Such information may be within Yinson but not to be leaked to anyone outside of Yinson).

c) Sensitive/Personal Data: Personal Data (categorized as sensitive or otherwise) protected by statutes, regulations, policies or contractual language which, if exposed or breached, could result in legal damages, fines/penalties, identify theft and/or financial fraud.(Examples, passports numbers, health records, salary details etc).

d) Open: Data that does not fall into any of the other information classifications. This data may be made generally available without specific information owner's designee or delegate approval. (Examples include, but are not limited to, advertisements, job opening announcements, catalogs, regulations and policies, publication titles and press releases.).

4.2 Classification measures

a) Yinson Employees who in charge of the management of relevant data ("Controller of Data") are responsible for labeling data with the appropriate classification and applying required and suggested safeguards.

b) Controllers of Data to implement the relevant Classification watermark in WORD or PDF documents (e.g. Confidential, Restricted etc.)

c) Controller of Data to label files in softcopy with the Classification label. Such files or drives should only allow access based on the level of Classification.

d) Controllers of Data should label physical files with the appropriate Classification label.

4.3 Internet Usage Policy

This Internet Usage Policy applies to all employees of the Yinson Group who have access to computers and the internet to be used in the performance of their work. Use of the internet by Yinson Employee is permitted and encouraged where such use supports the goals and objectives of the Yinson's Group's business. However, access to the Internet through the Yinson Group is a privilege and all Yinson Employees must adhere to the policies concerning Computer, E-mail and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Yinson Employees may also be held personally liable for damages caused by any violations of this policy.

4.3.1 Computer, e-mail and Internet usage

a) Yinson Employees are expected to use the internet responsibly and productively. Yinson Employees are advised to exercise good judgement and remain productive at work while using the internet.

b) Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.

c) All internet data that is composed, transmitted and/or received by the Yinson Group's computer systems is considered to belong to the Yinson Group and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

d) The equipment, services and technology used to access the internet are the property of the Yinson Group and the company reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

e) E-mails sent via the company e-mail system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

f) All sites and downloads may be monitored and/or blocked by the Yinson Group if they are deemed to be harmful and/or not productive to business of the Yinson Group.

g) The installation of software such as instant messaging, peer-to-peer (P2P) technology is strictly prohibited, unless approved by Yinson Group.

h) Unacceptable use of the internet by employees includes, but is not limited to:

   i) Access to sites that contain, terrorist organization affiliated, obscene, hateful, pornographic, unlawful, violent or otherwise illegal material.

   ii) Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via the Yinson Group's e-mail service.

   iii) Using computers to perpetrate any form of fraud, and/or software, film or music piracy.

   iv) Stealing, using, or disclosing someone else's password without authorization.

   v) Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.

vi) Sharing confidential material, trade secrets, or proprietary information outside of the organization.

vii) Hacking into unauthorized websites.

viii) Sending or posting information that is defamatory to Yinson Group, its products/services, colleagues and/or other third party.

ix) Introducing malicious software onto Yinson Group network and/or jeopardizing the security of the organization's electronic communications systems.

x) Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

xi) Passing off personal views as representing those of Yinson Group's.

xii) Promoting any views that cause political, social, racial and religious disharmony.

If a Yinson Employee is unsure about what constitutes acceptable or unacceptable internet usage, then he/she should ask his/her manager/department head for further guidance and clarification. Any user violating these policies is subject to disciplinary actions deemed appropriate by the Yinson Group.

4.4 Access Control Policy

a) The access controls required to meet the security objectives of the Information Security Policy. Access control management is paramount to protecting Yinson Group information resources and requires implementation of controls and continuous oversight to restrict access.

b) Confidentiality, Integrity, and Availability (CIA) are fundamental aspects of protection of systems and information, and are achieved through logical, physical, and procedural controls. It is vital for the protection of systems and information authorized users who have access to Yinson Group systems and information are aware of and understand how their actions may affect security and privacy.

c) Access control is established by imposing standards for protection at the operating system level, at the Application level, and at the database level. Access to Yinson Group computer systems will be based on the principles of “least privilege” and "need to know” and must be administered to ensure that appropriate level of access control is applied to users as well as system support personnel to protect Yinson Group information systems.

d) Administrative (also known as "root") access to systems is limited to Yinson Employees who have a legitimate business need for this type of access. Administrative access to network devices may be logged.

e) All access to Yinson Group systems and services are reviewed by Yinson Information Security team and updated on a periodic basis to assure proper authorizations are in place commensurate with job functions.

f) Access to electronically stored records containing information will be electronically limited to those staff having an authorized and unique login ID assigned.

4.4.1 Physical Access Controls

a) Information processing and storage facilities shall be located in secure areas, and protected by a defined security perimeter, security barriers, entry controls, and access controls to protect against unauthorized access, damage, theft, and interference. The relevant Information Security or Data Privacy Departments shall conduct physical security assessments of Yinson Group facilities, including offices, rooms, and IT resources. The assessments shall identify the perimeter for the secure area and apply the measures necessary for complying with Yinson Group policies, procedures, and standards.

b) Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing personal information should be required to sign in at a designated reception area where they will be assigned a visitor’s ID or guest badge unless escorted at all times. Individuals issued with visitor identification shall ensure they are clearly visible at all times while the individuals are in Yinson Group facilities.

c) Access cards, keys, or identification badges shall not be transferred, loaned, destroyed, duplicated, or marked in any manner by any individual other than authorized Yinson personnel. The loss or theft of any access card, key, or identification badge shall be reported immediately to the relevant Yinson HR or Admin personnel. Access codes shall be protected and not shared or communicated with anyone who has not been granted access to a secure area.

d) Secure areas are restricted to authorized personnel. When applicable, unauthorized personnel may be permitted to visit secure areas when escorted by authorized personnel. Recording equipment (e.g., mobile wireless devices and cameras) shall be restricted as required in secure areas. A logbook must be administered to monitor all visitors to secure Yinson area, and this logbook must be verified by the relevant administration executives of Yinson.

e) Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved person in any area where files containing personal information are stored.

f) Cleaning personnel (or others after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored.

g) Further physical controls shall be detailed under the Physical Security Policy.

4.4.2 Electronic Access

a) Access to Personal data shall only be granted if such access is necessary to fulfil authorized Yinson Employee or third-party duties and responsibilities. Access shall be to the minimum information necessary to perform the duties and responsibilities in accordance with the Yinson Data Privacy Policy and this Policy.

b) Yinson Group's Information Technology ("IT") team shall create a user access profile based on each user's role with Yinson Group. A record of all users with access privileges to Yinson Group's IT resources shall be maintained in accordance with Yinson Group's policies, procedures, and standards.

c) Each Yinson Department representative shall review user access rights, either as part of a regular security review or more frequently (as required) and may revoke or modify privileges when necessary.

d) Yinson Group's IT team shall ensure a formal user management process is in place, including user registration and password management process, for granting access to information and IT resources.

e) Yinson Group's IT team shall grant access to information and IT resources to the level required to perform specified role-related responsibilities.

f) All computers with an Internet connection or any computer that stores or processes personal information must have a recently updated version of software providing virus, anti-spyware, and anti-malware protection, installed and active at all times.

4.5 Password Policy

a) This policy supports the Yinson Group IT regulations to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards. This policy applies all users and administrators of the relevant Yinson computer/IT system.

b) All users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

c) Password policies are used to mitigate possible attacks against the Yinson Group IT infrastructure and the data held upon it. Use of long, complex passwords helps to mitigate attacks that attempt to guess passwords, and regular password changes to mitigate long term exploitation of any disclosed or discovered passwords.

4.5.1 Password selection

a) Users must select a password that is secure and difficult to guess. Passwords must not be something that can easily by guessed (avoid using your name, children or a pet's name, car registration number, football team, etc).

b) In accordance with security best practice the following rules are advised:

i) All passwords should have a minimum of eight characters.

ii) Each password must contain a combination of at least three out of four-character sets: uppercase characters (A through to Z); lowercase characters (a through to z); numerical digits (0 through to 9); non-alphabetical characters (e.g.! $ # % @ +); Consecutive or repeated running alphanumerical characters are nor advised.

iii) Previous passwords used must not be re-used.

iv) In addition, while not actively enforced by the password creation process, accounts created for use on external online resources must not use the same password for authentication for any Yinson Group's related matters.

4.5.2 Changing a password

a) Passwords must be changed regularly to mitigate the long-term exploitation of any disclosed or discovered passwords.

b) The frequency of password change is generally based on the privilege or access level of the account. Accounts with greater privilege or access should have their passwords changed more frequently. It is recommended those passwords are changed every 180 days. Yinson Employees with access to highly restricted or confidential information should change their password every 180 days.

c) If any password has been compromised or there is suspicion that it's been compromised, the said password should be changed immediately.

d) Passwords must not be inserted into email messages or other forms of electronic communication.

e) Multiple sign-ins with the wrong username or password will result in a locked account, which will be disabled for a period of time to help prevent a brute-force sign-in, but not long enough to prevent legitimate users from being unable to use the application.

4.5.3 Password use

a) Passwords are the mechanism used to protect the security of Yinson Group's systems and must be protected. Some of the following safe practices are advised:

i) Passwords must be kept secret.

ii) Passwords must not be written in a form that others could identify (e.g. writing passwords on postage notes and pasted on monitor/laptops/workstation area.).

iii) Passwords must not be stored electronically in a non-encrypted format.

iv) Passwords must never be shared with others.

v) Care should be taken to prevent anyone from watching you type your password.

vi) Passwords must not be revealed over telecommunications electronic mail and other forms of electronic communications.

vii) "Remember Passwords" feature is not to be used in any external applications.

viii) Passwords are not to be stored in ANY computer system (including a smartphone or similar devices) without encryption.

4.6 Clean Desk Policy

a) A clean desk policy is to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or a Yinson Employee leaves his/her workstation.

b) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

c) Computer workstations must be locked when workspace is unoccupied.

d) Computer workstations must be shut completely down at the end of the workday.

e) Any confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

f) File cabinets containing confidential information must be kept closed and locked when not in use or when not attended.

g) Keys used for access to confidential information must not be left at an unattended desk.

h) Laptops must be either locked with a locking cable or locked away in a drawer.

i) Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

4.7 Remote Access Policy

a) All remote access to Yinson Group computer, network systems and hardware must be authorized, approved and documented. Any access not authorized and approved is forbidden. All Yinson Employee are allowed to work out of office. To remotely access computers, that is only allowed for staff with relevant job functions (e.g. I.T. to support others).

b) Remote access to specific applications, systems, components and technology infrastructure shall only be granted to personnel with a legitimate business need. The level of access granted, and privileges assigned shall be limited to the minimum required to perform the assigned duties.

c) Yinson Employees and/or third parties authorized to utilize remote access shall ensure that unauthorized users are not allowed access to the Yinson Group network while utilizing these connections. All individuals, while accessing the Yinson Group network, with either company-owned or personal equipment, are a de facto extension of Yinson Group's network and therefore their machines are subject to the same rules and regulations as stated in any applicable Yinson Group policy.

d) All devices that are connected to the Yinson Group network via remote access must use the most up-to-date anti-malware software and be current on available patches. Security patches for installed operating systems (with auto-update enabled), web browsers, and common applications shall be applied in a timely manner. A personal security feature must be installed and enabled on each applicable device utilizing remote access.

e) Yinson Employees and/or third parties agree to apply safeguards to protect Yinson Group's information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remotely accessed data or services and to ensure the prevention of inadvertent or intentional viewing of displayed information. Third parties shall have to sign the relevant non-disclosure agreements before given any access.

4.8 Acceptable use of Information Technology Resources Policy

4.8.1 Purpose:

This Policy is designed to:

a) Ensure clear and consistent understanding of a Yinson Employee's or contractor's responsibilities when working with Yinson Group's information technology resources.

b) Outline the restrictions on using personal devices for business purposes.

4.8.2 Yinson Employee Responsibilities

a) Yinson Employees who use Yinson Group information technology resources are responsible for:

i) usage of the unique computer accounts which the Yinson Group has authorised for the user's benefit;

ii) selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer;

iii) using the information technology resources in an ethical and lawful way, in accordance with relevant legal requirements;

iv) ensuring the Yinson Group's information technology resources must not be used for unlawful, offensive or otherwise improper activities. For example, they must not be used for material that is pornographic, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening to stalk, bully, harass, defame or breach copyright;

v) creating, storing or exchanging information in violation of copyright laws;

vi) creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email;

vii) ensuring that except for limited personal use, IT Resources are only used for authorised purposes;

viii) notifying the Information Security team if they become aware that information technology resources are being used by any person to infringe the intellectual property rights of another person or Yinson Group, or that the effect of any use of any facilities is to infringe such rights;

ix) observing the Terms of Service or Acceptable Use policies of third-party products or services that have been engaged by Yinson Group.

4.8.3 Yinson Employees use of Yinson Group Devices/Resources

Yinson Employees who use Yinson Group issued devices are to adhere to the below requirements.

a) Whilst in possession of the device, Yinson Employees will at all times comply with the Yinson Group's Code of Conduct Policy, Information Security Policy, Data Privacy Policy, and all other related policies. It is the employee's responsibility to ensure that they are familiar with these policies located on the Yinson Group's web portal.

b) Yinson Employees will take all reasonable steps to safeguard devices and the information stored on it. This includes but is not limited to:

i) Not modifying the computer's operating system, installing unauthorised software, obtaining extra resources without authorisation, or allowing modifications or repairs to be taken by anyone other than Yinson Group IT team.

ii) Making the device available to Yinson Group IT staff as requested for periodic audits or upgrades to the hardware and software provided, as well as for other tasks.

iii) Keeping the device in a secure location when outside the office and when not in use, to prevent accidental damage. For example, an unattended locked car is not considered secure.

iv) Disallowing any other person to use the device unsupervised or passing on to any other unauthorised person any software, licences or resources installed on or associated with it.

v) If at any point you suspect that you may have opened a malicious resource, software, or email you must notify Yinson Information Security team support immediately.

4.8.4 Misuse of Information Technology resources

a) Misuse of Yinson Group's IT Resources is a breach of the Acceptable Use of IT Resources Policy.

b) Any member of the Yinson Group who becomes aware of possible misuse of Information Technology Resource must report it to either:

i) their supervisor or manager;

ii) the Human Resources Manager; or

iii) the Information Security Team.

c) In the event that misuse is determined by management, formal disciplinary action for staff will occur in accordance with the Yinson Group's policies and procedures.

4.8.5 Loss, theft, or damage processes

a) If a device is damaged, lost or stolen, the employee must report this to the Information Security team as soon as possible, within a maximum of 48 hours from the time of damage or loss was made known to the employee. A police report must be obtained if the device is stolen and provided to the Information Security team.

b) If through no fault of the employee, a Yinson Group device is lost, stolen or damaged, it will be repaired or replaced at Yinson Groups' expense.

c) However, if the employee contributed to the loss/theft/damage, then the employee may be asked, at the discretion of the relevant management, to contribute towards repair or replacement costs.

4.9 Bring your own Device Policy

a) Yinson Group recognises the benefits that can be achieved by allowing Yinson Employees to use their own electronic devices when working, whether that is at home, in office workstations or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD.

b) It is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing Yinson Group provided services on BYOD.

c) The use of such devices to create and process Yinson Group information and data creates issues that need to be addressed, particularly in the area of information security.

d) Yinson Group must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering Yinson Employees to ensure that they protect their own personal information.

4.9.1 Employee Responsibilities

a) Yinson Employees who make use of BYOD must take responsibility for their own device and how they use it. They must:

b) Familiarise themselves with their device and its security features so that they can ensure the safety of Yinson Group information (as well as their own personal information).

c) Invoke the relevant security features.

d) Maintain the device themselves ensuring it is regularly patched and upgraded.

e) Ensure that the device is not used for any purpose that would be at odds with this Information Security Policy.

f) The device specifications must be approved by Yinson IT.

e) While Yinson Group IT team will always endeavour to assist Yinson Employees wherever possible, Yinson Group cannot take responsibility for supporting devices it does not provide.

f) Yinson Employees using BYOD must take all reasonable steps to:

   i) Prevent theft and loss of data.

   ii) Keep information confidential where appropriate.

   iii) Maintain the integrity of data and information, including that on Yinson Group premises.

   iv) Take responsibility for any software they download onto their device.

g) Yinson Employees using BYOD must:

   i) Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.

ii) Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead they should use their device to make use of the many services that the Yinson Group offers allowing access to information on Yinson Group services securely over the internet.

iii) Where it is essential that information belonging to Yinson Group is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails.

iv) Ensure that relevant information is copied back onto Yinson Group systems and manage any potential data integrity issues with existing information.

v) Report the loss of any device containing Yinson Group data (including email) to the Yinson IT Help desk.

vi) Be aware of any Data Protection/Privacy issues and ensure personal data is handled appropriately.

vii) Report any security breach immediately to IT Helpdesk in accordance with the Information Security Policy (the Information Security team will be informed where personal data is involved).

viii) Ensure that no Yinson Group information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party.

4.9.2 Monitoring and Access

Yinson Group will not routinely monitor personal devices. However, it does reserve the right to:

a) Prevent access to a particular device from either the wired or wireless networks or both.

b) Prevent access to a particular system.

c) Take all necessary and appropriate steps to retrieve information owned by the Yinson Group.

4.10 Anti-virus/Software and Malware Protection Policy

Computer viruses are designed to exploit flaws or errors in software. These flaws or errors, known as vulnerabilities, can allow attackers the ability to gain access to and control a target computer which, in turn, becomes an entry point into the network. Desktops, laptops, servers, applications, and network devices can serve as access points to sensitive, personal and other confidential data. Security updates, patches, and anti-malware software are used and implemented by Yinson Group's IT team to protect and mitigate threats to the overall health of Yinson Group's network.

4.10.1 Virus Protection

a) All computers and fileservers connected to the Yinson Group's network shall be configured in accordance with this Policy as follows:

   i) All Yinson computer devices shall have the most recent version of anti-virus software that has been tested; and

   ii) All software shall be approved by Yinson Group's IT Team, installed, and actively running on these devices.

b) All Yinson computer devices shall be configured to automatically receive periodic virus definition file updates from centrally administered resources managed by Yinson Group IT.

c) All files on computer devices shall be scanned periodically for viruses.

d) Users shall not take action, without authorized approval, to exclude his or her computer from updates covered by this section.

e) An exception may be made by Yinson Group IT in instances where the virus protection software/other software interferes with a department's proprietary application processes and database structures. Possible examples of this would be vendor-controlled systems, or other validated systems, or devices where anti-virus software has not yet been developed. Prior to implementation of the nonconforming configuration, a waiver must be submitted to and signed by the Department Head responsible for the application/system and the relevant Information Security Officer (ISO). All exceptions must be mitigated by other forms of protection and require authorization from the Yinson's Group IT Team. Exceptions to this Policy may be allowed if the computer device cannot have anti-virus software installed as.

4.10.2 Patch Management

a) Yinson Group IT shall provide and maintain common software patches and updates for computing devices.

b) All computers and fileservers connected to the Yinson Group network must be configured to receive updates and patches from the centrally administered resource.

c) All patches which are to be deployed by Yinson Group's vendors shall be within a reasonable time in relation to the level of risk. Yinson Group IT shall prioritize vulnerabilities that represent an imminent risk the relevant Yinson office's computing environment. Any patches such as those that provide additional functionality or address performance issues, shall be completed as soon as adequate testing has been completed. Any patches that is of urgent importance relating to the security of Yinson Group network, must be approved by the Yinson IT team first.

d) If there is an active cyber incident, virus outbreak, or other critical issue that can be resolved with a security patch, Yinson Group's IT Team may direct its Yinson Employees to immediately deploy a patch to all relevant Yinson IT systems.

e) All new devices shall be patched to the current level, as defined by the operating system vendor, prior to the device being connected to the Yinson Group's network.

f) If the Yinson Group's IT are unable to provide required patching for certain applications, the application owner must develop a process for provisioning updates and ensure updates are deployed.

g) Patch management on systems running proprietary applications may require vendor certification of patches prior to installation that includes consideration of the underlying operating system.

h) In the event that a department requires an exception to a patch installation, any vulnerability shall be mitigated by other forms of compensating controls in consultation with Yinson Information Security team. The exception shall require an advance written waiver signed by the Department head responsible for the application/system and approved by the Yinson Group IT.

i) Yinson Group Information Security team shall periodically assess the security of the Yinson's Group's computer systems by conducting vulnerability assessments and penetration testing by scanning computing devices. Following these assessments, Yinson Group shall recommend security fixes or other compensating controls to improve the security of the computing environment.

4.10.3 Handling a Virus attack

a) When a Yinson Employee's device is discovered to be infected with any kind of Malware/virus, no action should be taken by the Yinson Employee and the relevant IT team personnel should be immediately notified to rectify the situation.

b) The relevant IT personnel should conduct the necessary tests to ensure if any data has been breached.

c) Yinson Group uses software from a variety of third parties, copyrighted by the software developer and, unless expressly authorized to do so, employees do not have the right to make copies of the software. The Licencing Policy is to respect and adhere to all computer software copyrights and to adhere to the terms of all software licenses to which Yinson Group is a party.

d) Also, Yinson Group is to manage its software assets and to ensure that Yinson Group installs and uses only legal software on its workstations and servers, in line with the detailed requirements from the relevant thirty party licensing requirements.

e) All End User Licensing Agreements have to reviewed before purchase, with Yinson Legal team if required.

4.11 Encryption Policy

a) Where possible all confidential, personal and restricted data must be stored on a secure Yinson Group network server with restricted access. Where it has been deemed necessary by Yinson managers to store confidential or restricted information on any device other than a Yinson network server, the information must be encrypted.

b) All confidential, personal and restricted data transmitted via email to an email address outside of the Yinson Group domain (i.e. one that does not end in "@yinson.com" or other Yinson domain) must be encrypted.

c) All passwords used as part of the process to encrypt/decrypt information must meet the requirements of the Yinson Group's Password Policy.

d) All laptop storage devices running Windows 10 are encrypted using Bitlocker provided by Microsoft.

e) Data files to be transferred to remote site have to be done using encrypted techniques (for example Secure FTP (SFTP) or WSFTP).

4.11.1 Servers

a) Confidential, personal, and restricted data stored on shared Yinson network servers which are situated in physically insecure locations (For example remote file/print servers) must be protected by the use of strict access controls.

4.11.2 Desktop Computers

a) Yinson Desktop computers are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed. However, the following types of Yinson desktop computers will need to have encryption software installed:

i) Yinson Desktop computers which are located in certain areas (for example: FPSO etc.).

ii) Yinson Desktop computers which are located in third party facilities.

The preferred method of encryption for Yinson Desktop computer devices is whole disk encryption.

4.11.3 Laptop

a) All Yinson laptop computer devices must have Yinson approved encryption software installed prior to their use within the Yinson Group. In addition to encryption, they must be password protected and have up to date anti-virus software installed.

b) The preferred method of encryption for laptop computers, is whole disk encryption.

c) Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential and restricted information.

4.11.4 Removable Storage Devices

a) All confidential, personal and restricted data stored on removable storage devices is advised to be encrypted and/or password protected. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

b) Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.

c) The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt and/or password-protect all confidential and restricted information stored on the removal storage device.

4.11.5 USB Memory Sticks

a) Confidential and restricted information are advised to be stored on Yinson approved encrypted USB memory sticks.

b) Yinson approved USB memory sticks are advised to be used on an exceptional basis where it is essential to store or temporarily transfer confidential or restricted information.

c) They must not be used for the long-term storage of confidential or restricted information, which must where possible be stored on a secure Yinson network server.

d) Confidential, personal and restricted information stored on the Yinson approved USB memory stick must not be transferred to any internal (except a secure Yinson network server) or external system in an unencrypted form.

4.11.6 Transmission Security

a) All confidential, personal or restricted data transmitted through email to an email address outside of the Yinson domain (i.e. one that does not end in “@yinson.com or other Yinson domain”) must be encrypted.

b) Where such data is transmitted through a public network (for example the internet) to an external third party, the data must be encrypted first or sent via secure channels (for example: Secure FTP, TLS, VPN etc).

4.12 Physical Security Policy

a) The purpose of this policy is to establish standards in regard to the physical and environmental security of the Yinson Group. All Yinson Employees, contractors and users with access to Yinson Group's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Yinson Group's equipment and the information that they use or manipulate.

4.12.1 Secure Areas

a) All Restricted, Confidential and personal information must be stored in secure areas protected by appropriate security controls.

b) A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored. Examples of secure areas for protection are:

i) A room with sensitive paper-based information;

ii) A machine room containing IT fileservers.

c) Physical security for Yinson Group premises must have appropriate control mechanisms in place for the type of information and equipment that is stored there, these could include:

i) Alarms fitted and activated outside working hours;

ii) Window and door locks;

iii) Access control mechanisms fitted to all accessible doors;

iv) CCTV cameras;

v) Staffed reception area; and

vi) Protection against damage e.g. fire, flood, vandalism.

d) As an example, access to secure areas such as the IT equipment rooms, must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should be ready to challenge anyone not known to them and/or not wearing a Yinson visitor pass. Each department must ensure that doors and windows are properly secured.

e) Yinson electronic cards, keys, (should be signed for/regularly audited) entry codes etc. must only be held by Yinson Employees authorised to access those Yinson premises areas and should not be loaned / provided to anyone else.

f) Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear a Yinson visitor pass. An authorized Yinson employee must monitor all visitors accessing secure Yinson Group premises at all times.

g) In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, and if the employee is suspected of deliberately or gross negligently causing the said breach or, if an employee of Yinson Group leaves outside normal termination circumstances; keys, badges, cards and other security related items should be recovered from the said employee and any door / access codes should be changed immediately, upon issuance of termination notice or the said breach.

4.12.2 Paper Based Data Security

a) Paper based (or similar non-electronic) information must be assigned an owner and a classification. If it is classified as restricted, personal, confidential, information security controls to protect it must be put in place. A risk assessment should identify the appropriate level of protection for the information being stored. Paper based information in Yinson premises must be protected by appropriate measures that could include:

iii) Filing cabinets that are locked with the keys stored away from the cabinet;

iv) Locked safes;

v) Stored in a secured area in Yinson Premises protected by access controls as per the Access Control Policy.

4.12.3 Equipment Security

a) All Yinson general computer/IT equipment must be located in suitable physical locations that:

i) Reduce risks from environmental hazards, for example, heat, fire, smoke, water, dust and vibration.

ii) Reduce the risk of theft, for example, if necessary, items such as laptops should be physically attached to the desk.

iii) Facilitate workstations handling sensitive data being positioned so as to eliminate the risk of the data being seen by unauthorised people.

b) Desktop and laptops PCs must minimize data stored on the local hard drive; data should be stored on the network file servers. This ensures that information lost, stolen, or damaged via unauthorised access can be restored with its integrity maintained. Information concerning network drives and the appropriate place to store Yinson information can be found on the intranet here.

c) All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from Yinson Group's IT Team.

d) All items of equipment must be recorded on an inventory. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.

e) All IT equipment must be recorded in the Yinson IT inventories using manufacturer's serial number.

4.12.4 Cabling security

a) Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

4.12.5 Equipment Maintenance

a) Yinson Group IT, all Departmental representatives and 3rd party suppliers must ensure that all of Yinson Group's IT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. Staff involved with maintenance must:

i) Retain all copies of manufacturer's instructions;

ii) Identify recommended service intervals and specifications;

iii) Enable a call-out process in event of failure;

iv) Ensure only authorised technicians complete any work on the equipment;

v) Record details of all remedial work carried out;

vi) Identify any insurance requirements;

vii) Record details of faults incurred and actions required;

b) A service history record of equipment should be maintained so that when equipment becomes older, decisions can be made regarding the appropriate time for it to be replaced.

c) Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs, for example equipment which are under a support and maintenance agreement.

4.12.6 Security of Equipment off Yinson Group Premises

a) The use of Yinson Group IT/computer equipment off-site must be formally approved by your line manager. Equipment taken away from Yinson Group premises is the responsibility of the user and must:

i) Be logged in and out;

ii) Not be left unattended;

iii) Concealed whilst transporting;

iv) Not left open to theft or damage whether in the office, during transit or at home;

v) Where possible, be disguised (e.g. laptops should be carried in less formal bags);

vi) Be encrypted if carrying personal or confidential information;

vii) Be password protected;

viii) Be adequately insured.

Users should ensure, where necessary and required that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported accordingly, losses or damage to equipment must be recorded.

4.12.7 Secure Disposal or Re-use of Equipment

a) Equipment that is to be reused or disposed of must have all of its data and software removed/destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools.

b) Software media must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

4.12.8 Delivery and Receipt of Equipment into the Yinson Group premises

a) In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied:

b) Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note.

c) Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.

d) Subsequent removal of equipment should be via a formal, auditable process.

5 CHAPTER V : INFORMATION SECURITY AWARENESS

5.1 Information Security Awareness and Training

Yinson Group requires completion of introductory and annually recurring security awareness training to ensure that all employees, contractors and third parties are familiar with information security policies, as well as departmental and local information security responsibilities.

5.2 Awareness Creation

The head of each department of Yinson Group shall lead by example by ensuring that information security is given a high priority. Yinson Group senior management shall ensure that information security communications are given priority by staff and shall support information security awareness programs. Yinson Group shall provide new employees and contractors with mandatory information security training as part of job orientation.

a) Yinson Group shall provide regular and relevant information security awareness communications to all staff by various means, which may include the following:

   i) Electronic updates, briefings, pamphlets and newsletters.

   ii) Self-based information security awareness training to enhance awareness and educate staff on information technology security threats and the appropriate safeguards.

   iii) An employee handbook or summary of information security policies, which shall be formally delivered to and acknowledged by employees before they access Yinson Group resources.

5.3 Training

All users of new systems shall receive training to ensure that their use of the systems is effective and does not compromise information security. The relevant Yinson department heads/managers/supervisors may train users on how new systems will integrate into their current responsibilities. Yinson Employees shall be notified of all existing and any new policies that apply to new systems.

6 CHAPTER VI : DATA BREACH RESPONSE

6.1 Data Breach Reporting and Response Plan

This policy sets out the processes to be followed by Yinson Employees and contractors in the event that they experience a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, information.

a) Accordingly, Yinson Group needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes a data breach that requires notification to the relevant parties and authorities.

b) Adherence to this policy will ensure that Yinson can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

6.2 Process where a breach occurs or is suspected

a) Where a data breach is known to have occurred (or is suspected) any member of Yinson Group and/or contractors who becomes aware of this must, within 24 hours, alert their head of department and Yinson Information Security team in the first instance.

b) The data breach information that should be provided (if known) at this point includes:

i) When the breach occurred (time and date).

ii) Description of the breach (type of personal information involved).

iii) Cause of the breach (if known) otherwise how it was discovered.

iv) Which system(s) if any are affected?

v) Which Yinson department/s is/are involved?

vi) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

A template can be found at Annexure A (Incident Response Form) to assist in documenting the required information.

6.3 Assess and Evaluate Impact

a) Assess and determine the potential impact. Once notified of the information above, the Information Security Team must consider whether a data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The relevant regional Data Protection Officer and the Chief Data Privacy Officer should be contacted for advice if personal data breach is involved.

b) Criteria for determining whether a data breach has occurred

i) Is personal information involved?

ii) Is the information of a sensitive nature?

iii) Has there been unauthorised access to information, or unauthorised disclosure of information, or loss of information in circumstances where access to the information is likely to occur?

iv) For the purposes of this assessment; please also refer to Yinson Data Privacy Policy for guidance.

6.4 Criteria for determining severity

a) The type and extent of information involved.

b) Whether the information is protected by any security measures (e.g. password protection or encryption).

c) The person or kinds of people who now have access.

d) Whether there is (or could there be) a real risk of serious harm to Yinson or any affected parties.

e) Whether there could be media or stakeholder attention as a result of the breach or suspect breach.

With respect to the above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation.

6.5 Information Security Team to issue pre-emptive instructions

On receipt of the communication/notification of the breach, the Information Security Team will take a preliminary view as to whether the breach (or suspected breach) may constitute a serious data breach (and in event of personal data breach, whether it should be notified to the relevant regulatory data privacy authorities). Accordingly, the Information Security team will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team). This will depend on the nature and severity of the breach.

6.6 Data breach managed by the Information Security Team

Where the Information Security team instructs that the data breach is to be managed at the local level, the relevant department must:

a) ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include retrieval or recovery of the information, ceasing unauthorised access, shutting down or isolating the affected system); and

b) submit a report to the relevant Yinson Admin Department within 48 hours of receiving instructions.

c) The report must contain the following:

i) Description of breach or suspected breach.

ii) Action taken.

iii) Outcome of action.

iv) Processes that have been implemented to prevent a repeat of the situation.

v) Recommendation that no further action is necessary.

The relevant Privacy Officer/Information Security team will be provided with a copy of the report and will sign-off that no further action is required.

6.7 Data breach managed by the Response Team

Where the Information Security Team instructs that the data breach must be escalated to the Response team, the relevant Information Security Team will convene the Response Team and notify the Senior Management of Yinson Group.

The Response team will consist of:

a) General Counsel (or nominee).

b) Head of Human Resources for the relevant Yinson office (or nominee).

c) Chief Data Privacy Officer (or nominee).

d) Head of IT (or nominee).

e) Head of Administration for the relevant office (or nominee).

f) Head of Corporate Communications (or nominee).

6.8 Primary role of the Response Team

a) There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

b) The following steps may be undertaken by the Response Team (as appropriate):

i) Immediately contain the breach (if this has not already occurred). Corrective action may include retrieval or recovery of the information, ceasing unauthorised access, shutting down or isolating the affected system.

ii) evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach;

iii) Call upon the expertise of, or consult with, relevant staff in the circumstances;

iv) Engage an independent cyber security or forensic expert as appropriate;

v) Assess whether serious harm is likely;

vi) (for personal data breach) Make a recommendation to the relevant Data Privacy Officer whether this breach constitutes a breach to be notified for the purpose of mandatory reporting to the relevant data privacy authorities and the practicality of notifying affected individuals.

vii) Consider developing a communication or media strategy including the timing, content and method of any announcements to the relevant regulatory authorities, staff or the media.

viii) The Response Team must undertake its assessment within 48 hours of being convened.

The Information Security Team will provide periodic updates to the Senior Management as deemed appropriate.

6.9 Notification

Having regard to the Response team's recommendation above, the information Security Team/Privacy Officer will determine whether there are reasonable grounds to suspect that a notifiable data breach has occurred. If there are reasonable grounds, the Information/Security Team must prepare a prescribed statement and provide a copy to the relevant regulatory authority (if needed) and other parties (if required) as soon as practicable (and no later than 72 hours after becoming aware of the breach or suspected breach).

A template can be found at Annexure B (Data Breach Response Form).

(For Personal Data Breach Only), If practicable, the Response Team must also notify each individual to whom the relevant personal information relates. Please refer to the Yinson Data Protection Policy for guidance.

6.10 Secondary Role of the Response Team

Once the matters related to the data breach been dealt with, the Response team should turn attention to the following:

a) Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training.

b) Prepare a report for submission to Senior Management.

c) Consider the option of an audit to ensure necessary outcomes are affected and effective.