CYBER SECURITY POLICY

1. INTRODUCTION

Objective

The objective of this policy is to provide foundation for preparing and protecting against cyber threats and other computer attacks.

Scope

This policy is applicable to all the users of information assets of the Company, including but not limited to, direct or contractual employees, business partners having relationship with the Company and people having direct or indirect access to the information database/network of the Company.

Policy

The Company understands that the effective use of data within the organization is critical to enhance the ability of employees and business partners to deliver more convenient and better services to the customers. The Company collects, uses, develops and stores a wide range of information which increases operational efficiencies, reduces costs and improves services and therefore it is important that data is managed as an asset and shall be protected from all kinds of cyber threats and challenges.

2. PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

The protection plan shall mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all departments for critical information, to reduce the risk of disruption and improve the security posture. The following protection measures shall be part of the plan:

Confidential data

Confidential data is secret and valuable. All employees are obliged to protect this data. Common examples include Unpublished financial information, Data of customers/partners/vendors, Patents, formulas or new technologies, Customer lists (existing and prospective), any other information which will adversely affect company reputation if unknowingly disclosed.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees should take assistance of IT personnel.
- Share confidential data over the Company network/ system and not over public Wi-Fi or private connection.
- Ensure that only authorized people or organizations have access to data.
- Report scams, privacy breaches and hacking attempts immediately or within 2 days of such incident.

Protect personal and company devices

When employees use their digital devices to access Company emails or accounts, they introduce security risk to our data. Employees are advised to keep both their personal and Company issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.

- Choose and upgrade a complete antivirus software. Install security updates of browsers and systems monthly or as soon as updates are available.
- Ensure they do not leave their devices exposed or unattended; Whenever employee leaves their desk, they should screen lock the digital device.
- Log into Company accounts and systems through secure and private networks only.
- Avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When new hires receive Company-issued equipment, they will receive instructions for:
    - Disk encryption setup
    - Password management tool setup
    - Installation of antivirus/ anti-malware software

They should follow instructions to protect their devices and refer to IT SPOC/personnel if they have any questions.

Keep emails safe

The Company shall use Office 365 outlook and Outlook Web Application (OWA) to email clients in the organization. Emails often host scams and malicious software (e.g. worms, trojans.) To avoid virus infection or data theft, employees are advised to:

- Avoid opening attachments and clicking on links when the content is not related to work (e.g. "watch this video, it's amazing");
- Be suspicious of clickbait titles (e.g. offering prizes, advice);
- Ensure that the names and email addresses of senders are legitimate;
- Never share email id and password with anyone else.

Any malfunctioning detected from the email id shall be the responsibility of the owner of that email id. IT manager shall be the custodian of the email id and he/she should maintain and review the consolidated list of email ids allocated to the users. In case of transfer or retirement of employees, email id shall be surrendered to the IT team/personnel/manager. The content of email will be deactivated or shared with successor after approval from reporting managers.

Unique account names and email ids shall be allotted to the employees and users shall not modify the security parameters within the Company email system. Any user making unauthorized changes to the email security parameters shall be subject to strict disciplinary action.

External or personal email ids shall not be allowed on the Company hardware and mass emailing shall be done through IT manager or with the prior approval of IT manager. The IT Manager must investigate promptly, resolve the issue and send a Company wide alert when necessary. IT Manager is responsible for advising employees on how to detect scam emails. We encourage employees to reach out to them with any questions or concerns.

Antivirus

All computers, laptops and servers must have a valid and updated copy of antivirus installed. The antivirus should be set to automatic updation mode for virus definitions which should be scheduled to open scan automatically and regularly, depending on the criticality, disk size, CPU loads and updating frequency. An infected machine should be immediately removed from the network. In case of known viruses the warning should be broadcasted in the whole organization.

Firewalls

The Company shall install network firewalls between internet and internal network system to establish a secure environment for the Company network and computer resources. This firewall shall filter internet

traffic to mitigate the risks and potential losses associated with security threats to the network and information systems.

The IT team is responsible for implementing and maintaining the firewalls and is also responsible for monitoring the real time incoming and outgoing internet traffic on regular basis. The firewalls shall allow only known and secured port on the Company network. Employees may request grant of port or service access to any workstation, which is blocked as per the policy. Such request must be pre-approved in writing by the department head and shall include a justification to support the request. The IT manager will evaluate the risk of opening the firewalls to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with the request is deemed objectionable then an explanation of the associated risks will be provided to the requestor and alternative solutions will be explored.

Whenever a new hardware, software or any other application is introduced into the Company network, the firewall setting shall be changed to accommodate such new implementation.

Unnecessary or Unauthorized Software

Software will be used only in accordance with its license agreement and any duplication of copyrighted software by the employees, unless otherwise provided in the license, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to the Company standards of business conduct. All the employees shall be prohibited to use such unlicensed software.

No employee shall use or distribute personally owned software which may threaten the integrity and security of the Company's IT assets Such freeware, shareware or Open source should not be used at any cost. Employees shall not download licensed software, which are available for a fee, without prior written approval of IT manager of the Company.

System Rights and Security Settings

Employees shall not be given right to install, remove, edit scripts and access of operating system source files, configuration files, and their directories without administrative review. The IT team shall assign minimum level of access permission to all system files. All the USB ports of the Company owned hardware shall be blocked or restricted for incoming or outgoing data.

Login Passwords

All access to a computer system must be controlled by an authentication method involving a combination of a Username and Password. The Username and Password combination must provide verification of the User identity. For this reason, employees are advised to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays);
- Remember passwords instead of writing them down.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Systems must be capable of sensing the password strengths intelligently and passwords must get blocked automatically, after three successive incorrect logins or failed login attempts and passwords may be re-enabled after raising a service request with IT manager/SPOC/executive.

Dual Factor Authentication

Dual factor authentication can drastically reduce the incidence of online identity thefts, phishing expeditions and other online frauds. The Company shall use dual factor authentication application and employees can access MS office 365 or other applications as recommended by IT manager, by using dual factor authentication application.

Web Content Filtering

IT manager shall define and configure rules to block any information passing through the filtering rules. It is based on the content of the website and shall be configured for all users, which shall allow only that website, which is relevant to the business requirements or which is completely secured. All user devices shall be synchronized with the policy governing machine for new category and policy update.

Software and Patch Updates

IT manager shall update system and software fortnightly to avoid the known attacks. The server should be updated weekly for any latest service packs and hotfixes. All the application software installed on server or workstation like web browser, should also be regularly updated with latest patches. All new software and patches shall be tested offline and then only put on the actual machines.

Encryption

Differentiating between data of little or no value and data that is highly sensitive is crucial when selecting and deploying an encryption solution. Encryption products should be selected based on the type of encryption they offer and the technical details of the system on which they will be installed. Commercial operating systems provide integrated encryption solutions at no additional cost. The Company shall use the integrated encryption solutions in combination with preferred third-party products.

Types of Encryption

Mobile systems such as laptops are highly susceptible to theft and frequently contain valuable data. Boot disk encryption requires the key in order to start the operating system and access the storage media. In this scenario the operating system is removed as a vector for attack in the event of physical compromise. Boot disk encryption is typically implemented in conjunction with full disk encryption. Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling with laptops or desktops that are not in a physically secured area.

Individual or multiple files and folders can be encrypted separately from the host operating system. These encrypted archives can be stored in different locations, such as network shares, external hard drives or can be transmitted securely via emailEmail-specific products integrate encryption into the client email, allowing messages and attachments to be sent in an encrypted form transparent to the user. This is most appropriate for departments whose users require frequent and regular encryption of email communications.

External devices such as hard drives, DVDs, CDs and USB flash drives can be encrypted in their entirety. Mobile devices such as PDAs and smartphones allow users to exchange, transfer and store information from outside of the office. The extreme portability of these devices renders them susceptible to theft or loss. The Company shall use standardized devices, such as laptops for storing, transmitting or processing sensitive data.

For transferring confidential data or financial transactions, digital signatures should be utilized.

Mobile devices need to be placed under Mobile Device Management (“MDM”). MDM will be utilized by IT department to monitor, manage and secure employees' mobile devices that are deployed across

multiple mobile service providers and across multiple mobile operating systems being used in the organization.

Prohibited usage

Certain usages are completely prohibited:

- Acquisition, storage, and dissemination of data which is illegal or pornographic.
- Pointing or hyper-linking of Company web site to other Internet/WWW sites, whose content may be inconsistent with this policy.
- Playing of any game on the Company owned hardware or network.
- Participation in any online contest or promotion.
- Sharing of the Company information or material on any publicly accessible internet computer, which supports anonymous FTP or similar services.
- Download of any inappropriate non-official material, such as photographs, music files, video files for personal use.

Third Party Access

When there is a proper business reason for a third party to be given access to the Company system or security domain, a risk assessment shall be carried out to determine security implications and control requirements. The Company shall identify and assess the risks associated with allowing third parties to access its information processing facilities and to implement appropriate controls. The controls shall then be agreed with the third party and incorporated into a contract with any relevant penalties for breach being clearly defined.

Training

The Company shall create a culture of cyber security and privacy, enabling responsible user behavior and action through an effective communication strategy. It should foster education and training programs to all the employees and business partners for awareness and skill development in key areas relating to cyber security.

Budget Allocation and Procurement

The Company shall allocate specific budget for cyber security initiatives and for meeting emergency response arising out of cyber incidents. It shall also include installation, strengthening and upgrade of information infrastructure with respect to cyber security and procuring trustworthy Information and Communication Technology (“ICT”) products and provide for procurement of indigenously manufactured ICT products that have security implications.

Risk Assessment

The Company shall create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security and encourage periodical tests and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in network. It shall address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

The Company shall mandate security audit of critical information infrastructure on a yearly basis.

Management Review

At any time and without prior notice, the Company reserves the right to examine emails, messages, files on laptops/Desktops and Tablets, web browser cache files, web browser bookmarks, and other information stored on or passing through the Company's computers. All transactions done over the Internet will be logged. These logged transactions will be used for analysis and can be audited further.

Reportable Incidents

Incident is defined as the occurrence of any situation which is inimical to this policy and which could compromise the confidentiality, integrity or availability of Information and Information Systems of the Company. Such an incident shall be immediately reported to the IT manager and Compliance Officer.

Disciplinary Action

Employees are expected to always follow this policy and those who cause security breaches may face disciplinary action.

In case of a first-time unintentional small-scale security breach, the company may issue a verbal warning and train the employee on security.

Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by- case basis. Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

CONTACT PERSON

IT Head

Email: helpdesk@asianet.co.id

Mobile: +6221 27098400

IT Manager

Email: helpdesk@asianet.co.id

Mobile: +6221 27098400

Compliance Officer

Email: ethic@asianet.co.id

Mobile: +6221 27098400