TITLE: **INFORMATION TECHNOLOGY SECURITY ADMINISTRATION POLICY**

REVISION HISTORY

REV	CHANGE DESCRIPTION	ORIGINATOR	DATE RELEASE
00	Initial Release	Edward Lee	29th April 2009
01	Update in IT Security Administration Policy	Edward Lee	11th Jun 2015
02	Update to Data Security Policy	Derrick Lee	8th Mar 2020

TITLE: **INFORMATION TECHNOLOGY SECURITY ADMINISTRATION POLICY**

Table of contents

TITLE: **INFORMATION TECHNOLOGY SECURITY ADMINISTRATION POLICY**

Section I. Foreword

Purpose and Objectives

All computer and data communications systems used to access company business sensitive information or that are critical in feeding information to the system must employ a formal security administration policy which is used to ensure that only authorized personnel gain access to company data.

IPS will expand this policy to other business critical systems at senior management's discretion. This includes safeguarding of all Digital Intellectual Property (IP) information received from clients.

The intention of this policy is to formalize the procedures for granting employees access to systems and ensure that access levels are maintained appropriately when employees change job functions. The policy will also ensure that unauthorized attempts to gain access to systems are identified and that a periodic review of users with access to systems is performed to ensure that the policies have been followed consistently.

Scope

Refer to Appendix A for a list of systems that must comply with the IPS Security Administration policy.

The security administration policy must be employed at the network, database, and at specific applications and databases levels for the systems listed in Appendix A.

The policy applies to all employees, contractors, temporary employees, or others who have a business need to access the company's systems.

Responsibilities

The ultimate responsibility for implementing and complying with this policy rests with senior management at IPS. Senior Management will designate the IT manager/System Administrator to implement and monitor this policy. The day-to-day implementation is the responsibility of the systems and data owners, whether they are part of the IT department or Operations who access to the systems.

Policy Revisions

This policy will be reviewed and revised as needed and on an annual basis. Approved and implemented by IPS management.

IPS Management is required to develop detailed policies procedures to meet the Corporate policy objectives on individual business critical systems listed in Appendix A. User Awareness training must be performed whenever there are significant changes to this or internal company policies procedures.

Section II. Policy Statement

Physical Access Control Policy

Systems should be physically secured from unauthorized access:

- Servers, telecommunications wiring closets, switches, etc. should be in locked areas accessed only by authorized IT personnel.
- Workstations should employ password protected screen savers or other means of locking the workstation when it is not in use.
- Backups of critical information should be stored off-site in a secure location.

IPS Implementation Procedure

All ERP Enterprise, Deployment, Mail, E-Business, Firewall and Network servers will be kept in a locked room. Entry is limited to IT staff and those allowed entrance by the IT Manager for the region.

Server rooms will be locked with a Finger Print Scan system, lock and key or with changeable combination. The network teams in each region will have the keys to access the Server rooms.

- All user workstations will have a time-triggered screen saver with password control. The users will be asked to change this password every 60 days. A recommended setting for idle time is 5 minutes.

Access Authorization and Control Policy

Access to company systems and data should be granted to users based on the user's job responsibilities and with the approval of the data owner manager.

- IPS will identify Regional Security Administrator(s) who will:
    - Monitor and enforce the network security policy.
    - Answer questions of data owners and users.
    - Monitor data owner and user compliance with the IPS security policies.
- Be a liaison with the department manager in ensuring that segregation of duties and other controls are effectively implemented in the IT environment.
- System access criteria will be developed, by job function, ensuring that only transactions and data required by the user can be accessed. This will maintain and control segregation of duties.
- IPS will employ a method of authenticating users with remote access to the Email system. Only approved user will be granted remote access to the Email mailbox using Web Access.
- IPS will maintain a physical or electronic documentation of a manager's approval for the level of access granted and for each change in access is required.

- When a user changes job functions, their access must be re-authorized by their new manager.
- A copy of all access authority documents should be maintained.

IPS Implementation Procedure

IT is responsible for ensuring that only authorized users of systems have access to relevant information, software, or network components.

Employees should regard security responsibilities as shared and should use sound judgment and common sense to ensure that Company data and systems are protected.

1. Report all suspected unauthorized attempts to IT.
2. Change passwords as required by Company policy.
3. Keep passwords confidential.
4. Do not write down passwords where they are openly visible or can easily be found.
5. Change passwords if it is suspected that someone else has obtained them.
6. Do not disclose passwords over the phone.
7. Passwords should be adequately complex, comprised of a combination of numbers and letters. Do not use names, birth dates or common words.
8. Users are responsible for all network access violations that result from sharing, displaying or not protecting passwords or not having password changed when necessary.
9. Unattended workstations should never be left logged on for an extended length of time or overnight.
10. Workstations left unattended for a brief length of time should be protected by a password enabled screen saver or approved security utility.
11. Laptops should never be left out overnight. They should be locked down to a stationary object using a locking device or placed in a locked drawer or cabinet Or locked office.
12. Any computer that is lost, stolen or compromised must be immediately reported to IT. Any account that is compromised must be immediately reported to IT. The user's password will be immediately changed or account locked to limit security threats.
13. Accessing intranets or email via pubic kiosks or PC's other than your own is not permitted. User ID and passwords are frequently cached in memory and introduce security threats. If use is necessary, either reboot the PC or close the browser when finished to avoid potential access to Company accounts.
14. Any security incident such as unauthorized access, malicious code (viruses), network intrusion or denial-of service attacks detected or reported, an incident response team consists IT manager, network and system administrator, HR security officer, Business unit manager and Financial controller, should be activated to isolate, investigate, recover and report the incidents to the top management.

Password Control Policy

User ID's and passwords should be used to authenticate users to all systems listed in Appendix A.

Passwords must not be shared.

- Passwords must be changed at least every 60 days.
- Network passwords that have not been used should be disabled after a maximum of 60 days.
- Minimum password length of six characters.
- Passwords should be comprised of numeric and alpha-numeric characters and should not include easily guessed words or numbers (names, birth date, user's initials, etc.)
- Passwords should be changed immediately if a user suspects that someone else has obtained their password.
- Passwords should not be written down where they could be accessed by another user.
- Passwords should be disabled after 5 failed attempts.
- IT intervention should be required to re-enable a user account. Record of the intervention should be forwarded to the IT Security Administrator.
- Terminals/PCs should deactivate after a maximum of 30 minutes of inactivity through system utilities or password screen savers.

IPS Implementation Procedure

Individual site shall maintain a set of the relevant administrator passwords and safe keep in the locked safe. The safe with passwords should be limited to the Senior/System Administrator and/or the IT manager of the facility. The safe should be fireproof in the event of a disaster.

Password changes must occur a minimum of every 60 days. Passwords must be a minimum of 6 characters in length. All server passwords should not be dictionary-based words, and local administrator password lengths must be a minimum of 6 characters.

Any passwords stored in the safe will be communicated across the team of System Administrator with an understanding that no modifications or changes to the regional network will be made without the authorization of the IT Manager.

Data Security Policy

Data that is considered confidential (i.e. employee data, business plans) should be stored in a secured servers. User ID and password information must be encrypted prior to being transmitted in the internet environment.

Web and FTP servers need to implement HTTPS (HTTP over TLS 1.2) or SFTP to ensure data is transmitted securely from one system to another system.

Data which belongs to customer in its digital form, known as Digital IP, includes digital files containing product keys, artwork, engineering specifications, bills of material and product images. Dedicated servers place onto dedicated segment of the network will be used to centralize the administration of the sensitive data.

All data containing Digital IP or PII (Personally Identifiable Information) needs to be encrypted with minimum AES-256 strength encryption algorithm.

Back-ups of confidential data should be kept in a secure environment. Back-ups need to be encrypted with minimum AES-256 strength encryption algorithm.

Controlling Access to Information and Systems

The most common threat to organizations comes from viruses, worms, and other hostile programming code. While it may be impossible to completely guard against all such threats, following the policies set forth here will minimize the threat potential.

The policy covers as below:

(1) Installing of hardware and illegal use of software is prohibited.

(2) Employees should know that they are not allowed to put any software on their PC whether for business or entertainment purposes without getting approval from IT Department.

(3) Employees are not allowed to access Company system and network using their personal devices. Namely, Laptops, PDAs, Mobile phones, Tablets and USB storage devices.

(4) Employees are not allowed to copy Company data from their company's PC to external websites or devices. Namely, Floppy drive, CD-Rom, CD Writer, DVD Rom, DVD Writer, and USB storage devices.

IPS Implementation Procedure

General purpose business data stored on the local file servers within the firewall. Digital IP data stored on dedicated Digital IP server place on a secure network path in the dedicated segment of the network within the firewall.

Access Level Maintenance and Monitoring Policy

The removal of access should occur when a user leaves the job function that they were assigned to through termination or transfer to another job function.

- Human Resources management should notify the System Administrator of job transfers and terminations.
- As an additional control, the Security Administrator will ensure that network access is removed for these employees if the employee terminated the service.
- The Security Administrator will notify all application and data owners of terminations of the employee and removal the access of the application system.

The creation of access should occur when a user request new account for accessing specific application system based on the assigned job function.

- Management will define and review critical application and database functions to ensure that access to those critical functions is limited to appropriate employees.
- System Administrator will grant access level privileges accordingly based on approved application.
- Only System Administrators are granted with admin privileges.

Unauthorized Access Attempt Policy

The System or Network Administrator must review failed or unusual access attempts to the system and report suspicious activity to the head of the IT department and their direct supervisor for further action.

- The review of access attempts should be documented on the access attempt log or in some other manner and retained for at least 2 years.
- Accounts with access to digital IP must be reviewed quarterly to validate that only authorized users have access to systems containing digital IP.
- Database systems should have audit features activated and activity logs reviewed periodically for unusual or unauthorized transactions.

IPS Implementation Procedure

All IPS network accounts will be created with a maximum of 5 failed login attempts. The account will be disabled once the fifth login attempt failed. The user will need to contact the IT help desk to reset the account.

User Awareness Training Policy

IPS is required to perform user awareness training on security. This training will provide users with enough information for them to understand why each of these security policies has been implemented and their requirements for following the policies.

User understanding and acceptance of these policies should be evidenced by the employee's signature on this policy that should be maintained in the employee's personnel file.

IPS Implementation Procedure

As part of the employee orientation program, new employee will be brief on the company IT security and operating policies. This includes awareness of the Personal Identifiable Information and vulnerability of network security.
The role of IT user support has expanded not only provide user access trouble-shooting but responsible to support external customer applications and to serve as the single point of contact for technical issues and handle security incident.
To provide support properly, the IT help desk is responsible for the following tasks:

a. Escalation guidelines.

b. Communication between the IT helps desk and application development groups.

c. Knowledge on the applications available to customers.

d. Brief users on security policies, procedures, and guidelines.

Section III. Appendices

Appendix A: Systems required to comply with this Policy

Systems that are required to fully comply with the IPS Security Administration policy are listed below. IT management at least once a year will update this list as part of the quarterly Information Technology Review to include all critical systems.

A. ERP System

Each user will be given a user profile limiting his/her access to only the transactions needed to perform his/her job. The department manager or senior management personnel must approve all new users request for account creation.

B. Systems access to servers contain Digital IP and PII (Personally Identifiable Information) contents

The above application systems or servers will fully comply with the Information Technology Security Administration Policy. The details are listed as follow:

- **Physical Access Control Policy** – The Senior/System Administrator is responsible for all servers.
- **Access Authorization and Control Policy** – The Senior/System Administrator is responsible for creating and maintaining all user accounts. This person will function as the Plant Network Security Administrator.
- **Password Control Policy** – The Senior/System Administrator is tasked to maintain all user profile and access level. The System Administrator is also tasked to monitor all unauthorized access.
- **Data Security Policy** – Data is stored on dedicated servers behind the firewall. Data is transmitted within the LAN/WAN private network. No users are allowed to remotely access to these servers. Data containing digital IP and PII must be encrypted with minimum AES-256 encryption strength.
- **Access Level Maintenance and Monitoring Policy** - The Senior/System Administrator is tasked to work closely with the Human Resources department to maintain an up-to-date list of active employees. The IT department is tasked to conduct a quarterly self audit of the active user list and access authorization.
- **Unauthorized Access Attempt Policy** – The Senior/System Administrator is tasked to create a monthly access log to monitor unauthorized access attempts. The application will be set to limit all accounts to five login attempts.
- **User Training Policy** – The System Administrator and IT Staff will coordinate all required user orientation training. All new users will be brief on employee orientation program and introductory training by the IT team.