e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

INSIDER THREAT MITIGATION MATURITY FRAMEWORK

1 INTRODUCTION

1.1 THE HUMAN BEHAVIOUR CHALLENGE

Insider threat is defined as the theft or leakage of information by Authorised users either with malicious intent or from accidental leakage.

Following is the list of these risky human behaviors which result in the realization of this risk:

1. **Transfer of information out of corporate network** using various mechanisms:
    a. **Portable Media** →Use of portable media such as USB sticks, SD Cards, portable harddisks etc to export information
    b. **Cloud Storage**→ use of dropbox, onedrive and other cloud distribution mechanisms
    c. **Corporate email** → Use of corporate emails to send information to 3rd parties.
    d. **Chats** → Use of chats to communicate information either file based or text based.
    e. **Websites**→Uploading information either text based or file based to various websites such as Facebook, blogs or web based chats
    f. **FTP** → Use of ftp and other specialized file transfer protocol based mechanisms
2. **Access of corporate information from non-corporate devices**. These include the following scenarios
    a. **Working from home**→ access of corporate emails. A user downloads sensitive information from the email to his house PC.
    b. **Mobile Phones and tablets**→Use of mobile phones to access corporate emails and saving information
    c. **VPN Networks**→ users using VPN networks to copy information out to their personal devices
3. **Accidental leakage of information** via theft or carelessness shown by authorized staff in the management of corporate information stored in corporate or non-corporate locations. Some of these scenarios are as follows:
    a. **Theft of devices** → mobile phones, portable media (USBs, SD cards etc) and laptops
    b. **Email, chat etc mistakes** → information sent out by mistake to wrong recipients
    c. **Sharing of home laptops and media** → sharing of home pcs with other family members results in the exposure of information by mistakes
    d. **Bad security on personal emails and cloud storage** → Information residing in personal user's cloud storage, emails etc is vulnerable to bad passwords which further runs the risk of exposing the information

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

4. **Retention of information by users who have left the company.** Information transferred by users to his personal devices and locations stays with the user
5. **Information passed to 3rd parties.** Information when passed to the authorized 3rd parties remains with them even when their contracts expire. Although these are usually covered by contracts but there is always a risk that if they are not careful or lack the means to secure this information, it might get leaked by their authorized users.

Traditional security's (example DLPs and web blockers) entire focus to this day has been to secure information and organization from unauthorized outside (hackers) or inside users and blocking them. Using this method to control authorized users without changing their behavior has failed as it is considered too troublesome as it has resulted in over blocking and in many cases has caused major hindrance to user's legitimate activities. The result of which this is that the authorised user are unblocked and from that point of view they are not monitored hence leaving the real sensitive information exposed.

1.2 MANAGING INSIDER THREAT USING A FRAMEWORK BASED ON HUMAN BEHAVIOR MANAGEMENT

The fundamental actor in the insider threat is the human factor. As such in order to handle this challenge a stage based approach is required which continuously improves the handling of sensitive information by changing the human behavior. This stage based approach is called as **Insider Threat Mitigation Maturity Framework.**

The framework starts from the point of view that security is everyone's business and each user has to take responsibility of his actions. Instead of **simply blocking** and saying this is allowed or this is not allowed it takes a softer approach based on human behaviour principals of **EDUCATE**, **TRUST** and **VERIFY**.

Following are the levels of this framework and related processes and sub processes which are adopted within organizations based on the maturity of their security management processes.

1) Level 1: Understanding the environment and user educations
2) Level 2: Decentralizing security enforcement to improve data classification and monitoring
3) Level 3: Securing and controlling information at the source via encryption

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

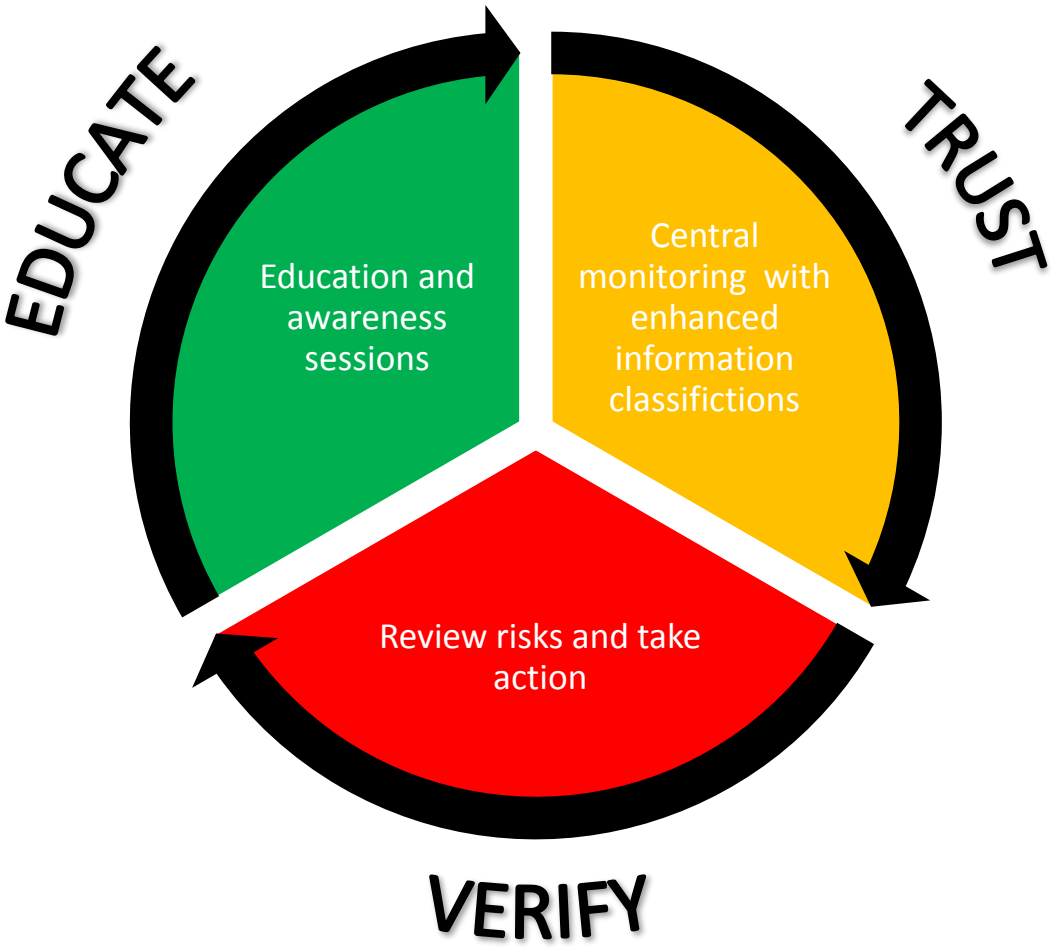
2 LEVEL 1: UNDERSTANDING THE ENVIRONMENT AND USER EDUCATION

The level has the following objectives:

1) Identify security risks posed by authorized staff due to out of ordinary behaviors such as copying large amount of files, copying information out of working hours etc
2) Eliminate risky behaviors by educating users such as the use of unauthorized applications (Shadow computing)
3) Establish standard operating processes for the use of specific sensitive information

The level involves 3 processes. Which are as follows:

1. ***Process (P1): Education and building awareness***
2. ***Process (P2): Central Monitoring to understand information usage and Identify Human Behavior Risks***
3. ***Process (P3): Review risks and take action***



e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

2.1 PROCESS (P1): EDUCATION AND BUILDING AWARENESS

Education is key in order to mitigate insider risk and is a continuous process. Users should be educated on how to handle sensitive information. Following are the ways this awareness is done:

1. **Information Owner/Top Management Briefings** → the sessions are targeted at top management and information owners in order to prepare them and get their commitment. Insider threat involves information owners taking more responsibility about their information and how it is being handled by themselves and their staff. This involves change and unless there is commitment among information owners the risk cannot be mitigated.
2. **End – User awareness sessions** →. Awareness sessions are key in educating the users on the dangers of various behaviours and the possible remedies that are be adopted. The awareness sessions should be held every quarter.
3. **Active reminders via policy screens on user logins** →Users should be reminded when they login about their roles and responsibilities on handling corporate information.
4. **Security Gap Analysis and Change Management Sessions to information owners** → Data from the human behavior monitoring activities is used to inform the information owners of their gaps. Ways of mitigating the risks are discussed and processes changes are agreed upon. The agreed change processes are passed down to end-users during the end-user awareness sessions. The sessions should be held every quarter.

2.2 PROCESS (P2): CENTRAL MONITORING TO UNDERSTAND INFORMATION USAGE AND IDENTIFY HUMAN BEHAVIOR RISKS

The objective of this process is to understand information usage and movement and baseline human behavior risks for the organization based on individual user and user groups using easy to manage central monitoring capabilities.

The process involves monitoring all means of information movement and usage whether it is online or office for the purpose of detecting risky human behaviors. This is achieved by defining **information classification rules** based on the following criteria:

1. Sensitive words
2. File names
3. Fingerprinting of sensitive information
4. Regular expressions

The defined rules allow admin to understand and baseline the inherent risk within the organization. The process involves producing weekly, monthly and quarterly reports of the information usage.

Monitoring coverage should involve the following scenarios:

1. Monitoring laptops and PCs for all online and offline usage
2. Monitoring of all file transfers whether on external media or online via ftp, cloud storage e.g. dropbox, onedrive etc

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

3. Locating and monitoring where information is stored with the corporate networks. This should include file servers as well as user's PCs
4. Monitoring of all communication media either corporate of personal e.g. gmail, chat, facebook etc
5. Monitoring of corporate emails via central servers so that incase users use their home PCs or mobile phones to forward information it can be monitored
6. Access logs of internal application and document usage by authorized staff
7. Coverage of laptops and devices even when not in corporate network
8. Monitoring of virtual environment e.g. citrix based operating environments
9. Monitoring server internet connection and usb ports
10. Monitoring information movement based on Compliance standards such as ISO27001, Privacy regulations etc
11. Usage and time spent by users on different online websites
12. Usage and time spent by users on different offline application
13. Installation of unauthorized applications

IT/IT security admin need to establish abilities to be able to cover all the above established monitoring areas.

Human behavior analysis should be done on the above scenarios to detect out of ordinary behaviours. For example a user copying large amount of files to his Dropbox when normally he copies only a few files. It is important the reports produced should be actionable reports with the following details:

1. User and PC/device detail
2. Clear detail of the information which was used or transferred

Outcome of this level are security gap analysis reports which should include the following

1. A summary of the identified risky or suspicious user behaviours
2. Full detail of the users and user groups involved in the risky behavior along with the detail of their actions.

2.3 PROCESS: REVIEW OF SECURITY EFFECTIVENESS AND COUNTER MEASURES

The process involves reviewing the output of the central monitoring process. The central monitoring process should produce 4 types of reports

1. Daily detailed reports per user and department for highly sensitive information to be passed to the information owners
2. Weekly detailed reports per user and department based on overall information usage to be passed to the information owners
3. Monthly detailed reports and monthly statistics to be passed to the information owners and top management
4. Quarterly human behavior analytics report. Using behavior trends to identify potential risky behaviours to be reviewed by top management and information owners.

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

In case of serious risk immediate action should be taken regarding concerned individuals. In other cases the recommendations for improvement are put forward to the Security Gap Analysis and Change Management Sessions held every quarter.

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

3 LEVEL 2: DECENTRALIZING SECURITY ENFORCEMENT TO IMPROVE DATA CLASSIFICATION AND MONITORING

The main objective of this level is to improve data classification and in turn improve information monitoring and security. The focus in level 1 is to eliminate obvious risky behaviours and suspicious activities it fails to pick up and alert in time when a specific sensitive information is miss handled. Such as a procurement executive copying yet to be published tender specs to his personal dropbox. Although level 1 will pick this up but considering the 100s of hits it might get overlooked by the observers.

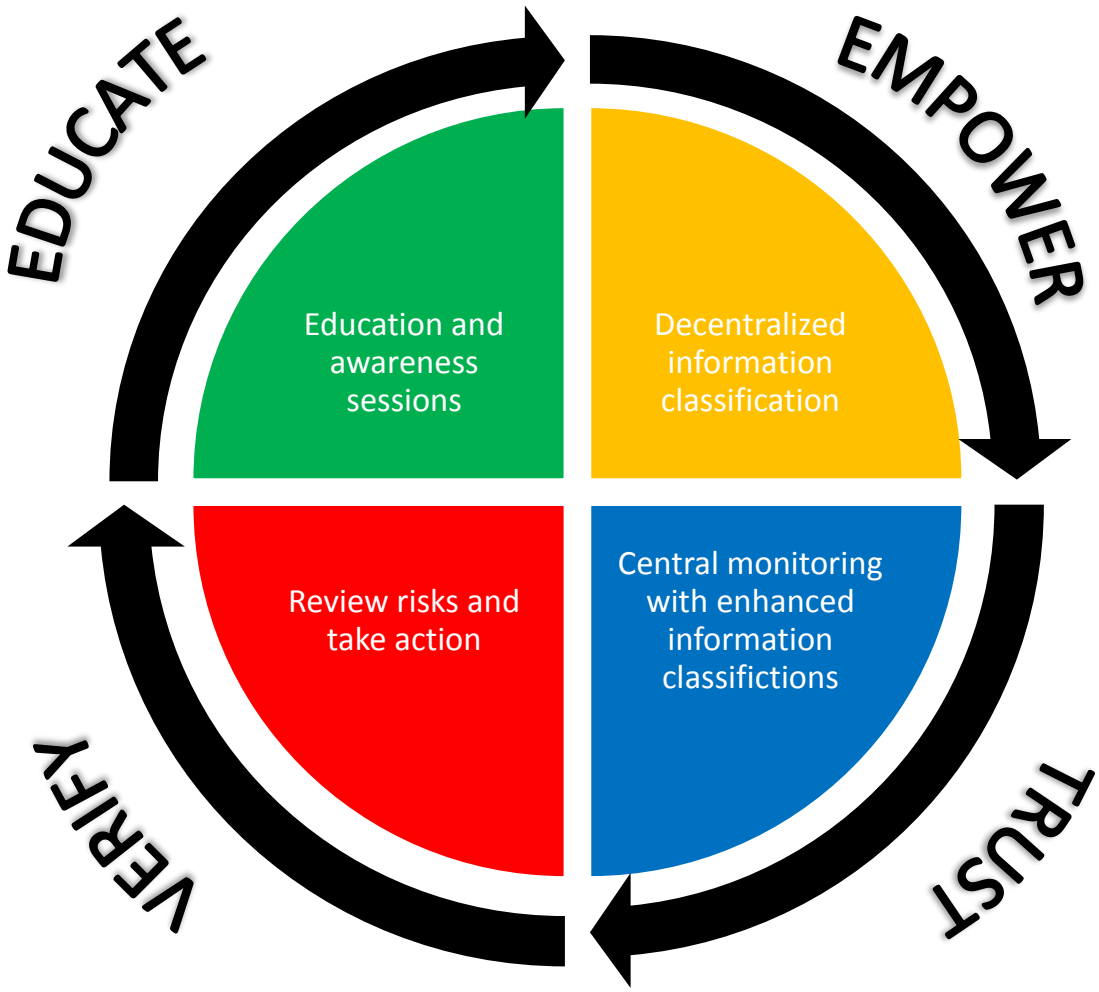
The level has the following objectives:

1) Improve data classification of adhoc sensitive information created by empowering the information owners to classify the information themselves
2) Reduce the detection time and effort by improved monitoring through targeted reports/alerts based on irresponsible or suspicious behaviors regarding the usage of specific sensitive information.
3) Eliminate risky behaviors by educating users on the use of specific sensitive information such as banning using dropbox etc to transfer yet to be published tender specs.
4) Establish standard operating processes for the use of specific sensitive information

The level adds 1 additional processes and 2 sub process to the existing processes. Which is as follows:

1) Process (P1): Education and building awareness
    a. ***Sub Process (P1SP1): Educating information owners on how to classify specific sensitive information***
2) Process (P2): Central Monitoring to understand information usage and Identify Human Behavior Risks
    a. ***Sub Process (P2SP1): Monitoring information based on decentralized information asset classifications***
3) ***Process (P4): Decentralized information classification by information owners***

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069



3.1 SUB PROCESS (P1SP1): EDUCATING INFORMATION OWNERS ON HOW TO CLASSIFY SPECIFIC SENSITIVE INFORMATION

In level 2 the main concentration is to decentralize information classification. This involves training information owners on how to classify sensitive information as they produce and use it. As such these trainings have to be made part of the education and training sessions.

3.2 PROCESS (P4): DECENTRALIZED INFORMATION CLASSIFICATION BASED ON INFORMATION OWNERS

The objective of the process is to better classify sensitive information which is usually created by information owners on an ad-hoc basis.

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

Information owners should be able to classify sensitive information as they create it based on the following attributes related to the specific information asset:

1) Sensitive words
2) File naming convention
3) Document coding convention
4) Fingerprinting information content
5) Transfer and usage restriction for the information asset
6) Authorised users for the information asset
7) Location of the sensitive information stores
8) Information sensitivity level
    a. Secret
    b. Sensitive
    c. Office use only
    d. General documents
9) Alert requirement
10) Expiry date for the information asset

The defined information classification about the information asset should be stored in the form of rules to be applied as part of the central monitoring system.

3.3 SUB PROCESS (P3SP1): MONITORING INFORMATION BASED ON DECENTRALIZED INFORMATION ASSET CLASSIFICATIONS

The sub process involves the application of the information asset classification provided by the information owners in the form of rules to the central monitoring system. This ensures that specific sensitive information can be differentiated when being monitored and subsequently alerted based on daily and weekly reports.

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

4 LEVEL 3: SECURING AND CONTROLLING INFORMATION AT THE SOURCE VIA PERSISTENT ENCRYPTION AND RIGHTS MANAGEMENT

The main objective of this level is to permanently prevent misuse of sensitive information even if it gets mishandled by users.

This is achieved by encrypting the information at the source using persistent encryption and rights management mechanisms. Persistent encryption means the information remains encrypted all the time even when accessed by the authorized users. At no time is the sensitive information available in an unencrypted format and can only be accessed on authorized devices. Further rights management ensures specific usage restriction (printing and copy pasting restriction) are applied on the sensitive information asset.

The level has the following objectives:

1) Educating users on the use of encrypted documents
2) Controlling and securing sensitive information throughout its lifecycle from the time it is created to the time its importance expires.
3) Controlling and securing information irrespective of whether it is accessed within corporate network or outside.
4) Controlling sensitive information when accessed by user's personal devices and in possession of 3rd parties without infringing any privacy laws.
5) Further improve data classification of adhoc sensitive information created by empowering the information owners to classify the information themselves
6) Improve information classified based on defined rules through a user feedback mechanism
7) Drastically reduce the monitoring effort and time by focusing only on information which is unencrypted or when the users remove encryption or package information to be sent to 3rd parties.
8) Establish standard operating processes for the use of specific sensitive information

The level adds 6 sub processes existing process. Which are as follows (highlighted in bold):

1) Process (P1): Education and building awareness
    a. Sub Process (P1SP1): Educating information owners on how to classify specific sensitive information
    b. Sub Process (P1SP2): Educating users on the use of encrypted sensitive information
2) Process(P2): Central Monitoring to understand information usage and Identify Human Behavior Risks
    a. Sub Process (P2SP1): Monitoring information based on new information asset classifications
    b. Sub Process (P2SP2): Encrypt sensitive documents based on the established rules and information classifications
    c. Sub Process (P2SP3): Defining roles and responsibilities and privilege levels
3) Process (P3): Review risks and take action

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

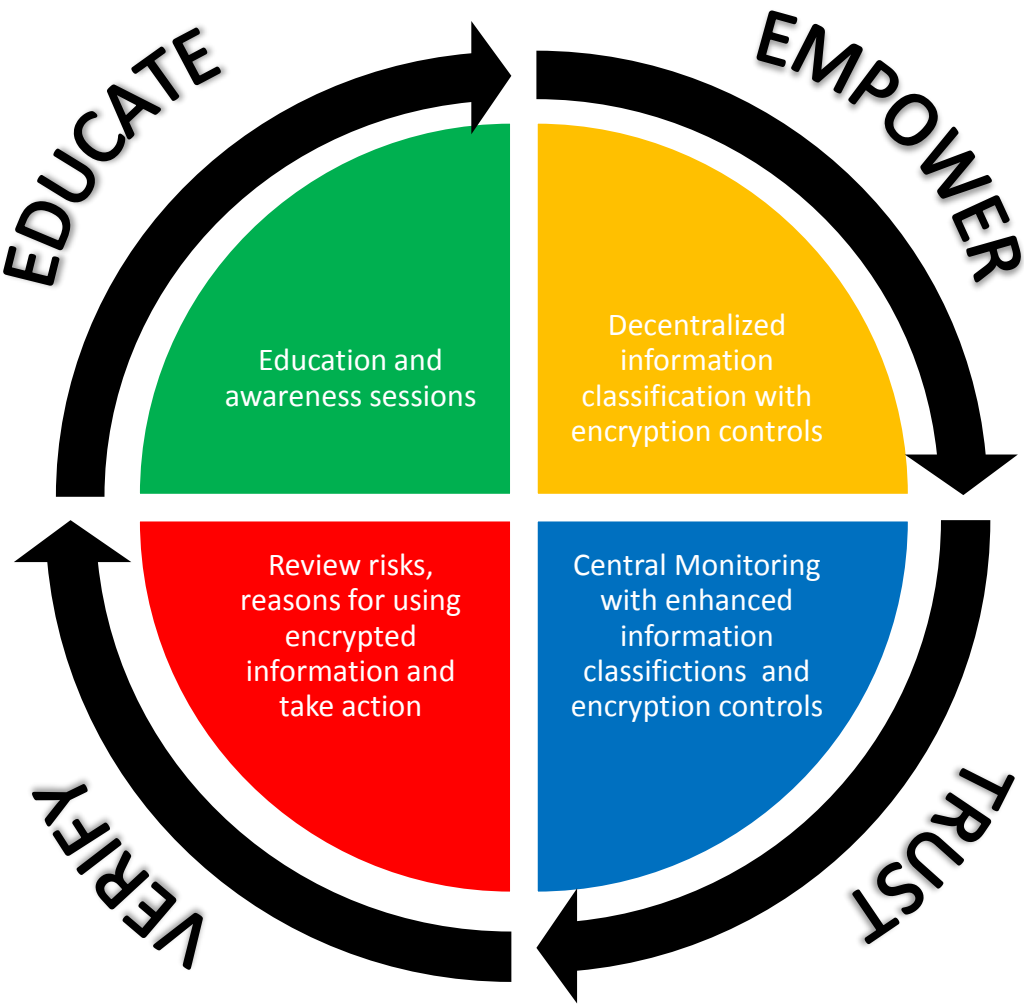
a. Sub Process (P3SP1): Monitoring information based on decentralized information asset classifications

b. Sub Process (P3SP2): Review of encrypted sensitive information usage reasons

4) Process (P4): Decentralized information classification by information owners

a. Sub Process (P4SP1): Adhoc classification of information by information owners

b. Sub Process (P4SP2): Overriding usage restrictions



4.1 SUB PROCESS (P1SP2): EDUCATING USERS ON THE USE OF ENCRYPTED SENSITIVE INFORMATION

The objective of this process is to educate users on how to encrypt sensitive information and what to expect once it is encrypted. The process involves different level of trainings for information owners who will create the sensitive encrypted information and those who will use the sensitive information. The process should cover the following areas during the training and awareness sessions with users:

1) How to identify different sensitivity levels of information (office use, sensitive, confidential etc)

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

2) How to work with encrypted information
3) How to encrypt sensitive information
4) How to restrict access of sensitive information
5) How to send encrypted information to 3rd parties while maintaining its security and encryption
6) How to send encrypted information to 3rd parties by removing encryption
7) How to ensure sensitive information is maintained
8) How to access sensitive encrypted information on personal devices such as home PCs and mobile phones.

4.2 SUB PROCESS (P2SP2): ENCRYPT SENSITIVE DOCUMENTS BASED ON THE ESTABLISHED RULES

The objective of this sub process is to extend central information monitoring and enforce encryption and rights management based on the defined information classification rules. The process involves applying the following controls:

1. Encrypting information based on defined information classification rules
2. Applying the correct usage controls based on the applicable sensitivity levels
3. Applying the correct user restrictions based on user groups
4. Auto encrypting all information based on user level irrespective of classification rules. For example devices of top management would contain highly confidential information some which might not be classified. This ensure end-end protection.

4.3 SUB PROCESS (P2SP3): DEFINING ROLES AND RESPONSIBILITIES AND PRIVILEGE LEVELS

With the ability to control information using encryption it is important to define who can do what and also their privilege level. The objective of the process is to define different roles and responsibilities for information owners and end-users and also deciding on their privilege levels. Following are the things to consider in the process:

1. Information usage controls based on user levels e.g. who can print what
2. Ability to encrypt sensitive information
3. Ability to restrict encrypted information
4. Ability to pass encrypted information to 3rd parties
5. Ability to access encrypted information from personal devices

4.4 SUB PROCESS (P4SP1): ADHOC CLASSIFICATION OF INFORMATION BY INFORMATION OWNERS

The objective of this process is for information owners to directly encrypt and classify information as they create it. This will ensure that there is no delay in securing the information. Information owners should be able to perform the following tasks:

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

1. Classify and encrypt sensitive information based different sensitivity levels
    a. Secret
    b. Sensitive
    c. Office use only
    d. General documents
2. Restrict access to the information to certain groups of users.

4.5 SUB PROCESS (P4SP2): OVERRIDING USAGE RESTRICTIONS AND TRUSTING THE END-USER WITH JUSTIFICATIONS

With the ability to classify and restrict usage of sensitive information it is important to provide flexibility in the usage of sensitive information based on **TRUST** as long as the user gives a reason for doing so. The objective of this process is to establish this process of user feedback when they are restricted in performing certain tasks. This might be due to wrong information classification for example a user is restricted from printing a certain document. On giving a reason the user should be able to proceed with the task. The reasons should be reported to the assigned information owner of the information asset for better classification of the information asset.

Apart from usage restrictions reasons should be requested from end-users during the following scenarios:

1. Sending out encrypted information to 3rd parties
2. Change sensitivity level of encrypted information
3. Changing access restriction of sensitive encrypted information

4.6 SUB PROCESS (P3SP2): REVIEW SENSITIVE INFORMATION USAGE REASONS.

With the ability to classify and restrict usage of sensitive information using encryption it is important to allow users the flexibility to continue with their tasks if they have genuine reasons for doing so. This is achieved by the user's overriding restrictions with a reasons.

The objective of this process is to review of the all the reasons posted by users of the information asset by the information owners. This check ensures that if the users are misusing the information it can be identified. Further the review also assists in verifying the applied security classification of the information asset and if it requires adjusting.

e-Safe Systems Sdn. Bhd. (865121-X)
www.e-safecompliance.com
L2-i-2, Enterprise 4, Technology Park Malaysia,
Bukit Jalil, 57000 Kuala Lumpur.
Tel: 03-89966061 FAX: 03-89966069

5 APPLICATION OF INSIDER THREAT MITIGATION FRAMEWORK

The application of the framework is a staged based process. Level 1 is the starting point and is deployed across the entire organization. Level 2 and level 3 require far more commitment from the information owners and end-users as such in order to reduce the amount of effort and change they can be rolled out to secure key information assets. This might be done by rolling levels 2 and 3 in certain key department of the organization first and once matured extending the coverage to the entire organization.