Information Security

Awareness Training
ISO/IEC 27001:2013

What is Information ?




An Asset that has value to the Organization
and that can exist in many forms
(written, spoken, sent, stored, printed, transmitted, …)





What is Information Security?

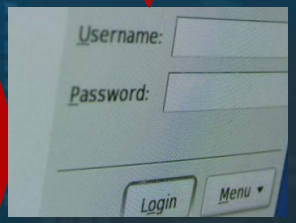
Confidentiality

Integrity

Availability

How do we practice “Confidentiality” ?

System passwords



welcome123

VS

W31(ome!@#

Clear desk clear screen policy

How do we practice “Integrity” ?

File permissions

✓ Read

X Write

X Execute

Document version and access restrictions

How do we practice “Availability” ?

Backup

Restoration

Information Security - Benefits

- ✓ *Protects information from a wide range of threats*
- ✓ *Ensure business continuity*
- ✓ *Minimizes business damage*
- ✓ *Maximizes business opportunities*
- ✓ *Gaines customer confidence.*

Key Drivers for Information Security

Technology

Security Tokens

Security Policy

Firewall

Audits

Process

Antivirus

ISMS

ISO 27001

People

Information Security is TEAM WORK

- It isn't just the sole responsibility of the security officer or the IT department.
- All the departments must be committed in protecting business information.

Why Security Breaches occur ?

- Lack of awareness on Policies & Procedures.
- Compromising security for convenience.
- Excessive dependency on technical controls.

Key Security Topics for End Users

- A brief snapshot of policies & procedures

Know the key people

S No	Member's Name	Organizational Role	ISSC Role
1			
2			
3			
4			
5			

Asset Classification

Classification	Description	Example
Restricted	This classification applies to the restricted business information, which is intended strictly for use within the organization or a group of individuals at the organization. Its unauthorized disclosure could adversely impact The organization, its employees, and/or its customers.	HR Employee records, invoices, and Internal audit reports, Designs, Project or Customer related information, etc.
Sensitive	This classification applies to all other information, which does not clearly fit into any of the other classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the organization, its employees / customers.	ISMS Policies, Procedures, ISMS manuals, Departments' SOP etc.
Public	This classification applies to information, which has been explicitly approved by the organization's management for release to the employees. By definition, there is nothing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.	Information available in the Internet sites, brochures, pamphlets, newsletters, press releases, Advertisements,Wall papers, Event results, Calendars, etc.

Please label your documents based on this classification

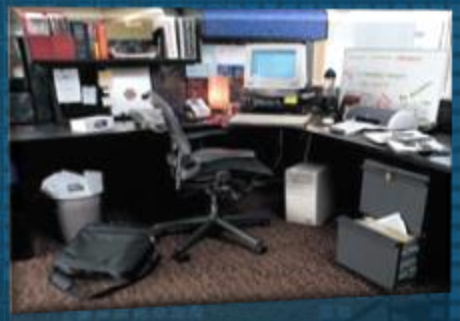
Physical Security

- Employees, visitors and vendors shall wear staff passes at all times in the company premises.
- Challenge any unknown person without proper identification such as a visitor pass.
- Tailgating/ Piggybacking is strictly prohibited.
- All physical security breaches should be reported to the physical security personnel.

Environmental Security

- Know your Fire evacuation procedures
- Know where are the emergency exits
- Learn how to use the fire extinguishers
- Assemble in the safe assembly area outside the premises for further instructions
- Attend fire drill sessions

Workstation Security



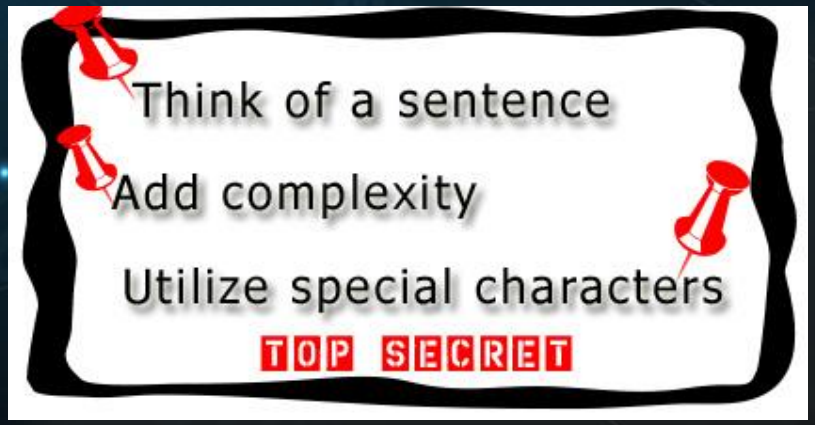
- Lock the work station when not in use.
- Installation of pirated or unlicensed software is prohibited.
- Collect all printout immediately from the printer area.
- All Sensitive documents to be cleared/shredded if not in use.
- All information on white boards to be erased after use.

Mobile devices security - Laptops

- While travelling, ensure that the laptop bag is physically secured. Secure it with a cable lock.
- While using restrooms at airports ensure your laptop is safe.
- Disable wireless auto-connection.
- Avoid insecure wireless connections in public places.
- Do not disable or ignore antivirus / patch updates.

Password Security

- Keep your password confidential at all times.
- Complexity: Minimum 8 characters long, with a combination of upper and lower case, numbers and special characters.
- Change: Once every 45 days – enforced by the system
- Change your password immediately if you suspect your password has been compromised.



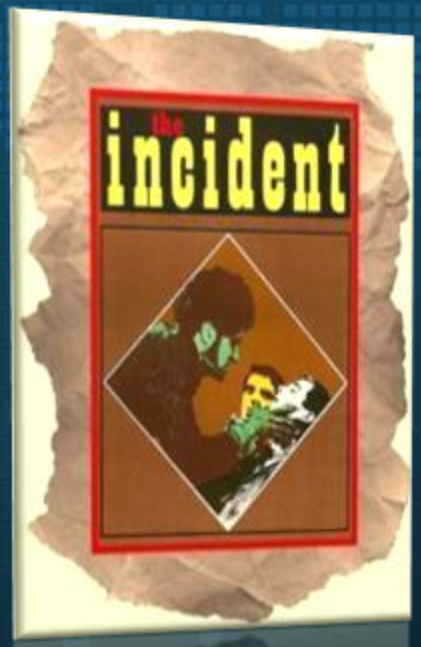
E-mail Security

- Email account should be used for **business purposes only**.
- Don't open attachments from untrusted senders.
- Create a strong email password.
- Do not save your email account passwords in web browsers.
- Do not forward chain/spam/junk e-mail.
- Use disclaimer notice to e-mails sent through company e-mail.
- Do not create or distribute any e-mail message containing offensive material to any person or organization using company e-mail.

Removable media security

- Authorization for usage of removable media is granted on “need-to” basis with prior approval.
- It should be used for **business purposes only**.
- Regularly scan the removable media for viruses.
- Media containing sensitive information must be completely formatted/ deleted/ demagnetized/ scrapped if no longer in use.

Information Security Incident



- All security events & weaknesses must be reported to the Information Security Team, incident response manager or directly to the CISO.
- Some common, incidents that one should report are:-
  - Password changes (you can't log in) or requests to share your password,
  - Workstation infection from a virus, worm or Trojan, adware, or spyware
  - Sudden workstation slowdowns,
  - File additions, changes, or deletions,
  - Access control door not functioning properly

- Beware of the threats around you

Security Awareness on Social Media -

LinkedIn, Facebook, Twitter, etc.

Social media is one of the fastest growing areas of online activity, and one of the fastest growing areas for malicious cyber activity. Even if your organization blocks access to social media sites, there are a tremendous number of risks you have to make your self aware of. Here are some of the key points we recommend concerning social media sites.

Privacy & Social Media:

- Privacy does not exist on social media sites.
- Yes, there are privacy options and controls, but too much can go wrong and your sensitive information can end up being exposed.
- Things such as your account being hacked, your friend's accounts being hacked, privacy controls changing, getting the privacy controls wrong, or people who you thought were your friends are no longer your friends.
- Long story short, if you don't want mom or your boss reading it--don't post it.
- This means being careful and watching what your friends post about you, including pictures. If nothing else, remember that employers now include sites like Facebook and Twitter as part of any standard background check.

Security Awareness on Social Media - LinkedIn, Facebook, Twitter, etc.

Scams & Social Media: Social media websites are a breeding ground for scams. If one of your friend's posts seems odd or suspicious, it may be an attack. For example, your friend posts that they have been mugged while on vacation in London and need you to wire them money. Or perhaps they are posting links about great ways to get rich, or some shocking incident you must see. Many of these scams or malicious links are the very same attacks you have been receiving in e-mail for years, but now bad guys are replicating them in social media. If you see a friend posting very odd things, call or text them to verify that they really posted the information.

Work & Social Media: Do not post anything sensitive about work. Be sure you understand your organization's policies about what you can and cannot post about your job.

Social media is a powerful way to communicate and stay in touch with people around the world. We do not want to scare people away from it. Instead we simply want to make people aware of the risks so that they can leverage technology more effectively.

Security Awareness on Social Media - LinkedIn, Facebook, Twitter, etc.

- The rules you must follow to avoid risks through social media.
  - When engaging online, do not post any confidential, internal-use only or copyrighted information .
  - Do not post anything that is offensive, harassing, or in violation of any applicable law.

Phishing

Examples of phishing email messages & links

- Phishing scams employ fraudulent e-mail messages or Web sites that try to fool you into divulging personal information.
- Phishing e-mail messages often include misspellings, poor use of grammar, threats, and exaggerations.
- To help protect yourself against phishing, use phishing filters, which helps in identifying and remove phishing attacks.

- Look forward to see you again……

The End

Thank You