Information Security

mediasystems
Powered by passion Steered by vision

Employees of MSI are expected to be familiar with MSI's Information Security Manual published.

This brochure is an introduction to Information Security.

Information Security

Information security refers to the controls that protect information assets from unauthorized access, destruction, modification and disclosure.

All staff members within MSI have a responsibility to protect its information and information processing technology as both are critical to the success of MSI corporate strategies.

Please report all security issues promptly to the Help Desk or Security Team.

Use of Desktops

All computers are the properties of MSI are provided for business use only. Be responsible for the security and proper use of your computer hardware, software and data.

Your access to MSI IT Systems is limited to that necessary to perform your job. You must not access information or systems that are not related to your business function.

Secure Password Selection

Since your password acts as a personal key, it provides access to computer systems and applications. It also gives each user certain permissions and capabilities.

To prevent passwords being easily guessed or cracked, ensure that strong passwords are selected, taking the following into consideration:

- Passwords must contain a minimum of 7 alphanumeric characters (a mix of upper and lower case) including at least one numeric character (e.g. **2BorNOT2b1**).
- Construct passwords that are not identical or substantially similar to passwords previously used (e.g. **dogsname1; dogsname2**).
- Use passwords that are derived from pass phrases (e.g., **Pemd0AS1 for " Please excuse my dear 0ld Aunt Sally1"**).
- Passwords must not be written down or recorded on-line in any form and passwords must not be shared with anybody.
- Do not use a word contained in English or foreign language dictionaries, spelling lists, or other common lists of words.
- Passwords must not be a user ID in any form
- Do not use industry or organization specific words (e.g. MSI)

For more details , Please read the password policy in our knowledge management site

Account Sharing

Do not share your computer account and password. You must not log in as anyone other than yourself, and you must not allow anyone to log in as you. Remember, you will be held responsible for all systems activity that is associated with your user account.

Unattended Workstations

Each employee is responsible for keeping his/her computer secure, including access to it. Lock your workstation every time you leave your desk.

Lock your PC using the following process:

- Hold **Ctrl, Alt & Del** keys down simultaneously. *Result: A Windows 2000 Security Dialogue box will appear.*
- Click on **Lock Computer** button.
  Result: Computer screen will now be locked.
- To log back into the PC, hold **Ctrl, Alt & Del** keys down simultaneously.
  Result: An Unlock Computer dialogue box will appear.
- Enter your network password and your PC will now be unlocked.

Remember to log out of your workstation and shut it off at the end of each day, unless business needs require that it be on. If your workstation is left on, make sure that it is locked and the monitor is turned off.

Internet Usage

If you are granted Internet access, ensure that the MSI connection to the Internet is used wisely. You must not violate any law, interfere with network users, services, or equipment, or harass other users. Remember that copyrighted material may not be duplicated or used in any manner that infringes on the copyright.

Downloading and uploading of software is not permitted, unless it has been approved by the appropriate IT Manager. For more details , Please read the internet and system policy in our knowledge management site

E-Mail Usage

E-mail has been provided as a business tool and must be used wisely.

You must not e-mail confidential information unless you encrypt the message. It is your responsibility to determine the confidentiality of each e-mail message you send.

Do NOT use email for any of the following:

- Illegal or destructive activities (e.g. the distribution of computer viruses);
- Personal gain, the conducting of outside business activities, political activity, fundraising, or charitable Activity not sponsored by MSI;
- Threatening or violent behavior;
- Gambling;
- Spoofing;
- Spamming (i.e. send bulk junk e-mails)
- Chain-letters;
- Personal announcements;
- Harassment or promoting harassment / Discrimination;
- Promoting personal, political or religious business or beliefs;
- Offensive or defamatory content (including pornographic literature or images) and,
- Broadcast messages without a specific company purpose.

Messages sent by outside parties must not be forwarded to third parties unless the sender clearly intended this and unless such forwarding is necessary to accomplish MSI business. If you forward or reply to a message you have received, do not change the original wording.
Be careful when addressing e-mail – know to whom you are sending the message..For more details , Please read the E-Mail policy in our knowledge management site

Virus Protection

Due to the increasing number of virus attacks and the speed at which the viruses can propagate through networks, you must take precautions to prevent any virus from entering and spreading within MSI environment.

Prevent the spread of viruses by adhering to the following:

- Not opening an e-mail message that is of a Questionable nature, such as an unusual attachment, a Message from an unusual sender, or unexpected e-mail; simply delete the message without opening it.
- Not opening any message that contains an executable file attachment (i.e. with an .EXE, .COM, .BAT, .DLL, .CMD, .VBS, .VBE or .PIF file name extension).
- Deleting spam, chain, and other junk e-mail without forwarding to other users

If you have any questions regarding the validity of an e-mail you have received or if you suspect a possible virus attack, contact the Help Desk.

Software Restrictions

Ensure that the following software restrictions are adhered to:

- Do not install any software onto an MSI computer or laptop.
- Users are explicitly prohibited from developing or using programs that attempt to bypass security mechanisms or which will undermine and weaken MSI systems infrastructure.
- Do not make unauthorized copies of software and comply with conditions that regulate the use of software utilized.

File Backups

Do not store any important information on your C:\ or D:\ drive as this information may be lost if the hard drive crashes or becomes corrupt.

By adhering to the standard process of storing important information on your personal network directory, this information is automatically backed up by the systems department.

Use the respective Share-Point portal to upload all project and process related documents

Physical Security

Ensure that the following physical control measures are adopted:

- Confidential or sensitive information in hardcopy form must be shredded before disposal
- Wear your photo ID tag at all times while at work.
- Challenge or report to security any unknown persons found within MSI premises.
- Ensure that all visitors are provided with visitor tags and prominently display these tags whilst on MSI premises.
-
- Keys and access cards are to be used only by the person they are issued to. Do not loan out your keys or access cards, and if they are lost or stolen report it immediately
- Do not allow unknown persons to “tail gate” through restricted doors.
- Lock cabinets that contain sensitive and confidential documents as well as diskettes, tapes or other media.
- All sensitive documents including BRD should not be left unattended.

Equipment Security

A few precautions that you must take to ensure that equipment security is maintained include the following:

- Use care in handling electronic equipment.
- Ensure that laptops, mobile phones and other portable electronic equipment are securely stored outside business hours.

Please read the internet and system policy in our knowledge management site

Monitoring of System Usage

You must be aware that MSI has the right to monitor the use by staff of MSI IT Systems and equipment (i.e. MSI management may read staff emails or may monitor internet usage). MSI may do this without notifying staff that monitoring is being conducted.

Disciplinary Action

If you do not comply with MSI policies, you may be subject to disciplinary action and in some cases, legal action or prosecution.

Information Security Contacts:

If you have noticed any security breaches or have any security concerns, please contact:

Incident Reporting: incidents@mediaus.com

Security Issues or Concerns?

Send an e-mail to: **ismg@mediaus.com**

If you have any concerns and issues adhering to the polices and procedure, Please contact our **HR manager**