



ISMS Excerpts – Resource Usage Policy & Password Procedure and Standards

YOUR RESPONSIBILITIES

- The employees of Aspire and other users authorized to use the resources of Aspire, understand and agree to unconditionally comply with the Resource Usage Policy.
- If there is any doubt about the ‘acceptability’ of use of company equipment, employees and other personnel should seek guidance from their manager / ISMS Officer.
- You are accountable for what you do on your system.

YOUR RESPONSIBILITIES

- Users are expected to access only those Aspire information assets for which they are authorized and as needed for their business purposes, maintain professionalism in all communications consistent with the Code of conduct.
- Users shall notify the immediate superior / ISMS Officer and report an incident in the Help Desk, when they notice any suspected misuse of Aspire information assets or security event or incident.

Users accessing Aspire's information assets understand and agree that Aspire rights include:

- The right to store, monitor, review, retrieve, destroy, log, audit and share data and information relating to:
 - Access and use of Aspire information assets, information and communication systems and facilities
 - Activities on the network domains of Aspire's computers, laptops, mobile devices, e-mails, instant messaging systems, voice based systems and other such services, whether or not required for legal, contractual and regulatory purposes.
 - All personal information stored, transmitted or being transmitted within Aspire's Information assets and resources
 - All hardware, software, systems and facilities to ensure compliance with its policies and procedures
- The right to block, terminate, and modify privileges for any kind of access or privileges with regard to the access and use of Aspire's information resources without any prior notice.

DEALING WITH COMPANY INFORMATION

Do



- Maintain in strict confidence all information or data or methods or techniques or any other information relating to Aspire or its customers or any other stakeholders.
- Respect copyright and trademark rights of the respective owners and adhere to terms and conditions of any and all software, database licensing agreements.

Do not



- Do not share any information or information resource relating to Aspire or its customers or any of its stakeholders, in any form or media (internet, email, etc) except for purposes explicitly authorized by Aspire.

“Information Security is Everyone’s Responsibility”

GENERAL SYSTEM USAGE GUIDELINES

Do



- Log off before you leave your workstation and lock your work stations whenever you leave your seat.
- Inform Help Desk immediately if you think that your workstation may have virus.
- Install / uninstall software with the help of the Help Desk.

Do not



- Do not commit system resource requirements to the customer without getting consent from the Help Desk.
- Do not share your login password with others.
- Loading unauthorized or untested software, i.e. pirated software or software not purchased through the formal purchasing process is forbidden.

“Information Security is Everyone’s Responsibility”

ELECTRONIC MAIL USAGE GUIDELINES

Do



- Include a meaningful subject line in your message.
- Check the address before sending a message and check if you are sending it to the right person.
- Delete electronic mail messages when they are no longer required.

Do not



- Do not send large messages, attachments, festive greetings, non-work items, chain or pyramid messages through email.
- Do not use e-mail for personal, non-business related communication
- Do not store any confidential attachments from official email account in your personal devices.
- Do not forward any official mails to your or others personal IDs.
- Do not download file attachments from public email services.

“Information Security is Everyone’s
Responsibility”

FILE STORAGE USAGE GUIDELINES

Do



- Store all local files under E:\<UserName>
- Store working project related files and knowledge documents in the centralized folder under P:\<Project Name>

Do not



- Do not save any unwanted or non-project related files in the Project folder (P:\<Project Name>)
- Do not share any folders in your workstation
- Do not share software with others (e.g. using the software installed on another system)

“Information Security is Everyone’s Responsibility”

INTERNET USAGE GUIDELINES

Do



- Use internet in an effective, ethical and lawful manner
- Use internet to obtain official business and technical information pertaining to Aspire

Do not



- Do not use Internet for video/audio downloading/streaming and for non-business related activities.
- Do not leave live internet feeds open all day to collect news or sports results.
- Do not make repeated attempts to access sites that are automatically blocked.
- Do not deliberately access sites containing pornographic, offensive, obscene or illegal content.

“Information Security is Everyone’s Responsibility”

DOWNLOADS (FTP AND WEB) USAGE GUIDELINES

Do



- Contact help desk to download a file of size greater than 5 MB.
- Use FTP scheduler when you are expecting to receive large files and schedule the download in the early morning before 6:00 AM.

Do not



- Do not download text or images which contain material of a pornographic, racist or extreme political nature.
- Do not download images, video or audio streams for non business related purposes

“Information Security is Everyone’s
Responsibility”

INTRANET USAGE GUIDELINES

Do



- Access business applications that are hosted on the intranet.
- Publish information deemed appropriate for the business.

Do not



- Do not make your password available for others to access intranet and intranet resources.
- Do not use someone else's user ID and password to access /update any information on the various Intranet systems.
- Do not publish information that has not been agreed as appropriate for the business.
- Do not deliberately update any part of the Aspire's intranet systems with incorrect data either for individual gain or to cause difficulty for the users.

**“Information Security is Everyone’s
Responsibility”**

INSTANT MESSENGER USAGE GUIDELINES

Do



- Login to Lync first thing in the morning.
- To use public instant messenger services for customer interaction, send a request to help desk with an approval from your project manager.

Do not



- Do not use public instant messenger services

“Information Security is Everyone’s Responsibility”

COMPANY TELEPHONES AND FAXES USAGE GUIDELINES

Do



- Communication in connection with company business
- Occasional personal use if deemed necessary and with the prior agreement of the manager

Do not



- Do not make / receive regular calls of a personal nature from your or someone else's telephone.
- Do not send / receive personal messages through official fax machines.
- Do not use company telephones to conduct business activities other than those connected with Aspire.
- Using company telephones and fax machines for purposes of a discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libelous or defamatory nature is forbidden.

“Information Security is Everyone’s
Responsibility”

GENERAL GUIDELINES

Do



- Use company supplied software and store data in connection with normal business
- Use communication devices for business purposes
- Limit the amount of personal data stored on your device so that it does not interfere with normal performance.
- Print what is necessary in the course of business.

Do not



- Do not install any hardware without the prior consent of your IT Department.
- Do not leave confidential or sensitive printouts uncollected from the printer.
- Storing / printing unauthorized copyright content in any form is forbidden.
- Printing or storing files or software containing pornographic, offensive, obscene or illegal content whether text, image, video or audio format is forbidden.

“Information Security is Everyone’s Responsibility”

APPLICATION AND DATA USAGE GUIDELINES

Do



- Execute/perform business processes as per your job function.
- Using your ID on systems approved for use.

Do not



- Do not make your password available for other people to use on your behalf.
- Do not use the password of another person.
- Do not copy or attempt to make copies of applications, systems and data unless expressly authorized by your manager in writing.

“Information Security is Everyone’s Responsibility”

EXCHANGE OF INFORMATION - ONLINE TRANSACTIONS

Do



- Check for site safety. Look for the padlock symbol on the bottom bar of the browser to ensure that the site is running on secure mode before you enter sensitive information.
- Clear your browsers cache and history before and after each session so your account information is removed.
- Review your bank and credit card unbilled transactions regularly to make sure that these transactions have been made only by you.

Do not



- Do not click on links from mail.
- Disable “Auto Complete” on your browser.
- If you get an email that looks like it's from your Internet Service Provider or someone else with whom you have an account asking to confirm your password, don't respond until you've checked with the company directly.
- Do not store the passwords / PIN on your computer or desk where others might easily find them.

“Information Security is Everyone’s Responsibility”

TELECOMMUTE GUIDELINES

Do



- You are responsible for the safety and security of all company property and proprietary information.
- Adhere to the terms and conditions of employment and relevant client's agreements at the telecommute location.
- You must use software, software utilities, equipment and electronic networks belonging to Aspire or the customer only for the purposes of carrying out the assigned work.

Do not



- Do not access Aspire or Customer network through VPN from Public Internet Café.
- Do not save the Email password when prompted in the browser from Public Internet Café.
- Do not copy any confidential/sensitive files/folders to/from Aspire network through VPN.
- Do not encourage your team members to use your credentials to connect to VPN under any circumstances.

“Information Security is Everyone’s Responsibility”

PASSWORD CONSTRUCTION STANDARDS

Passwords should contain the following characteristics to be considered as strong:

- Should contain both upper and lower case alphabets
- Should contain digits and special characters in addition to alphabets
- Should be at least eight to twelve alphanumeric characters long
- Create passwords that can be easily remembered
- Passwords should not have information identifying you like names of family and friends, birthdays and personal information.
- Passwords should not contain any computer terms and word or number patterns

“Information Security is Everyone’s Responsibility”

PASSWORD PROTECTION STANDARDS

- Do not use the same password for Windows, Outlook, and Outlook express accounts as for other non-Aspire access
- Do not share passwords with anyone
- All passwords are to be treated as sensitive, confidential information.
- Do not hint at the format of a password
- Do not reveal a password on questionnaires or security forms

“Information Security is Everyone’s
Responsibility”

PASSWORD PROTECTION STANDARDS

- Do not reveal a password to co-workers while on vacation
- Do not create a password file to store passwords, unless encrypted
- Do not use the "Remember Password" feature of applications
- If an account or password is suspected to have been compromised, modify the password immediately.

“Information Security is Everyone’s
Responsibility”

