Datamatics
Business Solutions

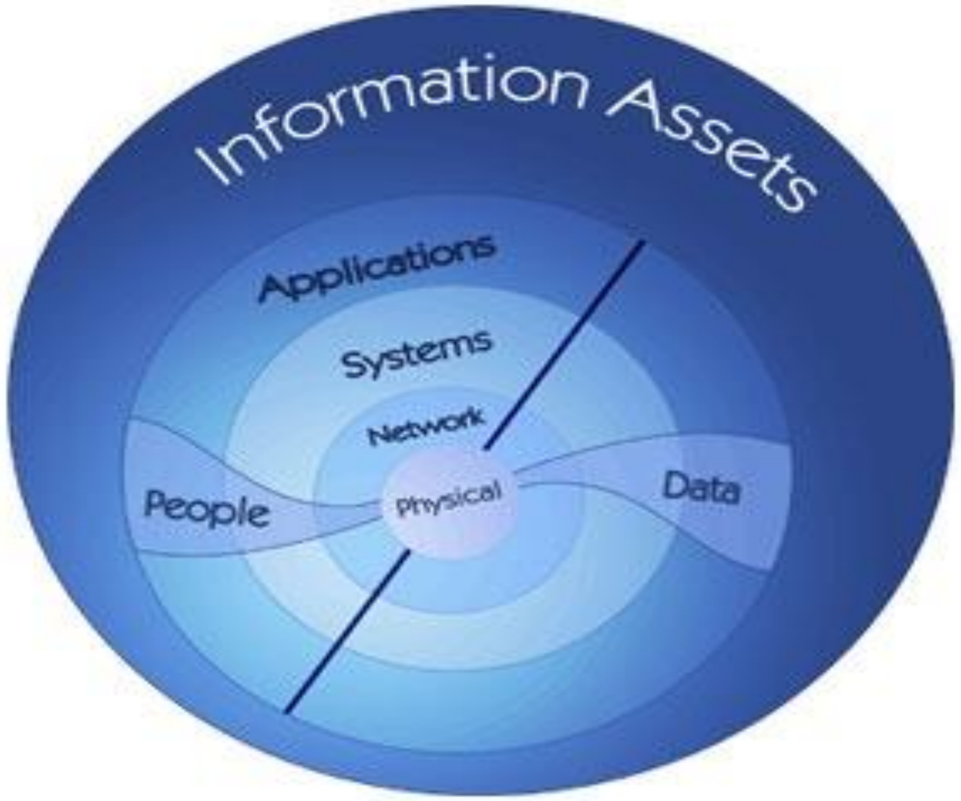
ISMS – INFORMATION SECURITY AWARENESS TRAINING

INFORMATION

Information is an asset, which, like any other important business asset, adds immense value to an organization due to its critical nature and hence needs to be suitably protected. Whatever form information takes, or whatever the means by which it is shared or stored, the need to protect it cannot be underestimated.

Types of Information

1. Printed or written on paper
2. Stored electronically
3. Transmitted by post or using electronics means
4. Published on corporate website
5. Verbal – spoken in conversations



© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION SECURITY

Information systems security

“The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.”

© Datamatics Business Solutions Ltd. All rights reserved.

DATAMATICS ISMS POLICY STATEMENT

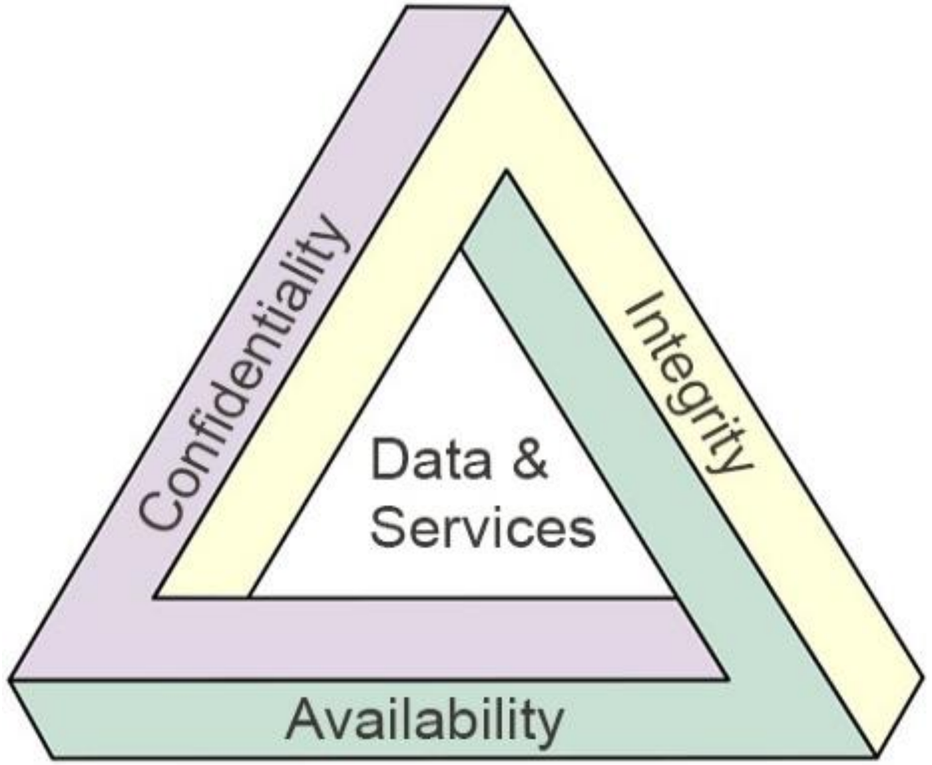
“We are committed towards developing and implementing an Information Security Management System (ISMS). Our Information Security Management System includes protection of Information against any unauthorized access, assuring Confidentiality, Integrity and Availability of information and compliance with legislative and regulatory requirements through business continuity plans, information security training and awareness, adoption of systematic approach to risk management, continual improvement.”

© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION SECURITY CHARACTERISTICS

C I A

Confidentiality (C): Ensuring that access to information is appropriately authorized.
Integrity (I): Safeguarding the accuracy and completeness of information and processing methods.
Availability (A): Ensuring that authorized users have access to information when they need it.
In addition, other properties are the Authenticity, Accountability, Reliability and Non-Repudiation



Protect, detect, and recover from insecurities.

© Datamatics Business Solutions Ltd. All rights reserved.

THREATS ACTORS

The possible threats to Information Security are:

- Computer-assisted fraud
- Espionage
- Sabotage
- Vandalism
- Fire or flood – Natural Calamity
- Computer viruses
- Computer hacking or malicious software
- Denial of service attacks

© Datamatics Business Solutions Ltd. All rights reserved.

SECURITY BREACHES LEAD TO…

- Reputation loss
- Financial loss
- Intellectual property loss
- Legislative and Regulatory breaches leading to legal actions (Cyber Law)
- Loss of customer confidence
- Business interruption costs

LOSS OF GOODWILL

© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION SECURITY MANAGEMENT SYSTEM

An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, business processes and also includes IT systems.

© Datamatics Business Solutions Ltd. All rights reserved.

ISO27001:2013 – INFORMATION SECURITY STANDARD

“A proven framework to initiate, implement, maintain and manage information security within your organization”

- Developed by ISO (International Organization for Standardization).
- Management framework that provides a model to establish, implement, operate, monitor, review, maintain and improve information security within the organization.
- Applicable to all sectors of industry & commerce and not confined to information held on computers.
- Addresses information security in whatever form it is held
- It takes a Risk Management approach
- PDCA (Plan-Do-Check-Act) cycle

© Datamatics Business Solutions Ltd. All rights reserved.

ISO27001:2013 – INFORMATION SECURITY STANDARD

Features:

- ✓ An internationally recognized structured methodology dedicated to information security.
- ✓ A comprehensive set of controls comprised of best practices in information security.
- ✓ 114 Controls in 14 groups.

A.5: Information security policies
A.6: Organization of information security
A.7: Human resource security
A.8: Asset management
A.9: Access control
A.10: Cryptography
A.11: Physical and environmental security
A.12: Operations security
A.13: Communications security
A.14: System acquisition, development and maintenance
A.15: Supplier relationships
A.16: Information security incident management
A.17: Information security aspects of business continuity management
A.18: Compliance

© Datamatics Business Solutions Ltd. All rights reserved.

COMMON INFORMATION SECURITY MYTHS

- Information Security is not my responsibility.
- I don’t have anything to contribute to Information security.
- My job doesn’t involve anything related to InfoSec.
- I know all to know about InfoSec.
- Not to report any incident. /exceptional situations to your managers and Premise Security officer.

© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION SECURITY IS EVERYONE’S RESPONSIBILITY

- Report information security events or incident immediately to the concerned authority.
- Run antivirus scans regularly.
- Take Backup of data frequently.
- Shred hard copies of Confidential. information retaining the Original copies.
- Lock your computer and mobile phone when not in use.
- Ensure that unauthorized persons do not view Confidential Information on your system while working.
- Do assume that Information Security is relevant to you.

- Click on links from an unknown or untrusted source.
- Install unauthorized programs on your work computer.
- Use Public Wi-fi hotspots and avoid working in public places in the first place.
- Disclose your password to anyone.
- Leave your computers unlocked when left unattended.

© Datamatics Business Solutions Ltd. All rights reserved

DATAMATICS'S OBJECTIVE – ADHERENCE TO ISMS

- To build an effective management framework for managing Information security with Datamatics.
- Ensure Information assets are handled effectively based on the risk rating.
- Develop a cycle for continually improving Information security within Datamatics processes.
- Compliance with Globally recognized standard.
- Ensure compliance with various government legislations and regulations.
- Create strong adherence to Datamatics's Policies and procedures.

© Datamatics Business Solutions Ltd. All rights reserved.

HOW DO WE PROTECT US

- With the Use of Policies, Procedures, Best Practice Guidelines.

- Policies that would help prevent loss of Data:

- ✓ Physical Access Policy
- ✓ Antivirus Policy
- ✓ Email Policy
- ✓ Internet Usage Policy
- ✓ Licensing Policy
- ✓ Backup Policy
- ✓ Incident Management Policy
- ✓ Change Management Policy

© Datamatics Business Solutions Ltd. All rights reserved.

PERSONALLY IDENTIFIABLE INFORMATION

- **What is PII?**

  PII is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.
- **Why is it important to safeguard PII?**

  Leakage of PII could lead to individuals getting exposed to many crimes, and could lead to business loss.
- **What is a privacy incident?**

  Breach of PII is considered as a privacy incident.

Responsibility of the departments

HR Staff members and Operations team are expected to be aware of the PII that they handle and ensure that it is reasonable secured.

© Datamatics Business Solutions Ltd. All rights reserved.

PII BEST PRACTICE

- Keep soft copies of PII in a safe location.
- If the soft copy is transmitted over USB pen drive / DVD / CD-ROM, ensure proper encryption technologies are used.
- Ensure that hard copies are retained in a secured location and access to the same is restricted.

- Do not leave print outs related to PII lying on your desk.
- Do not share PII with anyone without the need to know.

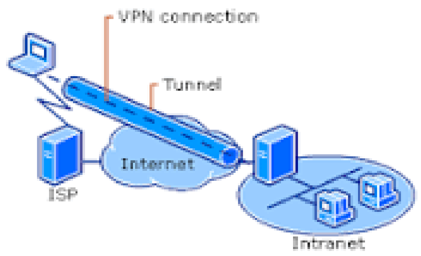
© Datamatics Business Solutions Ltd. All rights reserved.

DATA ENCRYPTION

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can with a key to decrypt.

- Data that is sent out on CD / DVD / USB / FTP should be encrypted.
- Access the web applications should be through the use of secure protocols like HTTPS only.
- All critical files / folders stored locally on the machine should be encrypted.
- Business critical data on the laptops should be encrypted.

- Do not send CD / DVD / USB drives outside the office premise without encrypting the data.
- Do not transfer critical data using unsecured protocols like FTP, HTTP, Telnet etc.



© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION CLASSIFICATION

All Datamatics information should be classified in the following three categories

- **Compliance**
  - Applies to information having clients Personally Identifiable Information and/or or Sensitive Personal Information (PII/SPI), the unwanted disclosure of which can bring penal consequences or damage to company's reputation.
- **Confidential**
  - Applies to sensitive business information that is intended strictly for named individuals such as merger and acquisition documents, information security strategy and corporate level strategic plans, human resources data, source code and vendor contracts.
- **Internal**
  - Information that is meant to be disseminated within the organization or a section of the organization such as company telephone directory, new employee training materials such as newsletters.
- **Public**
  - Information that is available to the general public and intended for distribution outside the organization such as product and service brochures, advertisements and financial statements.

© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION CLASSIFICATION (CONTD..)

- The classification level shall take into consideration the information’s legal requirements, sensitivity and criticality to the organization.
- All unclassified information shall by default be treated as “Internal” and shall be protected from unauthorized disclosure to a third party.
- All information shall be periodically reviewed and reclassified, if required by respective asset owners.
- On reclassification, all known users of the information shall be kept informed.
- Ensure that all the information assets are classified as per Datamatics’s Information Classification Scheme.

© Datamatics Business Solutions Ltd. All rights reserved.

WHAT IS SOCIAL ENGINEERING?

- **Social Engineering** is art of gaining access to information by exploiting human psychology, rather than by breaking in or using technical hacking techniques.
- Can be done through:
  - Direct human interaction
  - Social media sites / emails

Examples:

- **Phishing** - Used to deceive users and exploits the poor usability of technologies to acquire sensitive information such as usernames, password and credit card details- Bank Messages.
- **Dumpster diving** - Going through the trash.
- **Shoulder Surfing** - Looking over a shoulder to see what they are typing.
- **Mail attachments** - Programs can be hidden in e-mail attachments.

© Datamatics Business Solutions Ltd. All rights reserved.

SOCIAL ENGINEERING BEST PRACTICE

- Remember that passwords are sensitive. A password for your personal account should be known ONLY to you.
- Verify authenticity of unsolicited calls, visits or emails before responding.
- Take note of your surroundings to ensure that no one is shoulder surfing.
- Always escort the visitors.
- Use shredders to dispose off the paper documents containing confidential information.
- Cut up cards.
- Be Skeptical.

- Never give away information about yourself unless you have verified the identity of the party that is requesting it.
- Never open attachments in emails from unknown senders.
- Do not discuss confidential information in Public areas.
- Don’t click on links in emails. Type or paste them into your browser window manually to avoid phishing scams and Trojan infections.
- Do not respond to ANY Email message with personal information.

© Datamatics Business Solutions Ltd. All rights reserved.

ACCEPTABLE USAGE

- Utilize Datamatics information resources for business purposes only.
- Follow a clear desk and clear screen policy.
- Confidential information should be shared using a secure means of communication.
- Limit usage of external services such internet for business purposes only.
- Ensure all the employees of the vendor sign the "confidentiality agreement”.

- Do not share folders on laptops or desktops with confidential information unless authorized.
- Never leave your laptop bag unattended while traveling (Cars, airports, hotel rooms etc.).
- Don't permit 3rd parties to connect their devices to Datamatics network without approval.

© Datamatics Business Solutions Ltd. All rights reserved.

ASSET TAGGING

- **What is an Asset?**
  - Something possessed by a business entity from which future economic benefits may be obtained.
  - In InfoSec terms Asset is any data, device, or other component of the environment that supports information-related activities.
- **What is Asset Tagging**
  - Applying a label to an asset for security, inventory, maintenance and operational purposes.
- **Benefits of Asset Tagging?**
  - To prevent theft and enhance security of asset.
  - To maintain compatibility of assets for conformity.
  - To better manage the asset.
  - To meet the compliance requirements.

All Assets should be tagged as per Datamatics's Asset Management Policy.

© Datamatics Business Solutions Ltd. All rights reserved.

ASSET SECURITY

- Lock your workstation before leaving your desk: **“Press Ctrl + Alt + Del and Enter “ or “Windows + L”.**
- Make sure that encryption mechanism is installed on your laptop.
- Make sure that antivirus is up to date by checking the small Shield near the date and time tray on the right hand side of your computer.
- Report loss of desktop components, laptop, mobile devices, data-cards to your supervisor immediately.
- Data Cards should be used with appropriate authorization by authorized personnel only.

- Do not leave laptop or mobile devices unattended
  - In office
  - While travelling
- Do not connect smartphones to laptop to transfer any information or vice versa.
- Do not Connect storage devices like USB, hard drives without approval

© Datamatics Business Solutions Ltd. All rights reserved.

PHYSICAL ACCESS CONTROL

- All visitors must make an entry in the visitor register.
- All employees shall display identity badges throughout his/her stay in the office premises.
- Disclose your IT belongings especially laptops, pen drives, external hard disks while entering and going out of Premise, to the security personnel.
- Storage media and documents should be locked when not near your work area.
- Use shredders to dispose paper documents containing company information. Do not dispose them in dustbins.

- Avoid Tailgating. Swipe your cards ever time you access a restricted area.
- Do not enter the secured work areas without appropriate authorization.
- Hazardous material is not permitted inside the premise.
- Do not smoke, drink or eat in the proximity of your computing devices.
- Do not leave any documents unattended on the printers.
- Do not take any equipment inside or out of the premise without authorization.

© Datamatics Business Solutions Ltd. All rights reserved.

PROTECTION AGAINST VIRUS

- Scan files received on email or from internet before executing.
- Exercise caution when downloading files from the Internet. Download files from a legitimate and reputable source.
- Scan removable media like USB's, floppies etc. for virus before use.
- Inform IT helpdesk if your virus definition files are not getting updated regularly.
- Check that AV is installed on your machines.
- Check for the McAfee icon in your desktop system tray.

- Do not open email attachments received from an unknown source.
- Do not visit any suspicious websites.
- Don't download anything unless your current antivirus program installed on your computer is updated.

No anti-virus software can protect us from a New virus!

But your Alertness can

© Datamatics Business Solutions Ltd. All rights reserved.

PASSWORD SECURITY

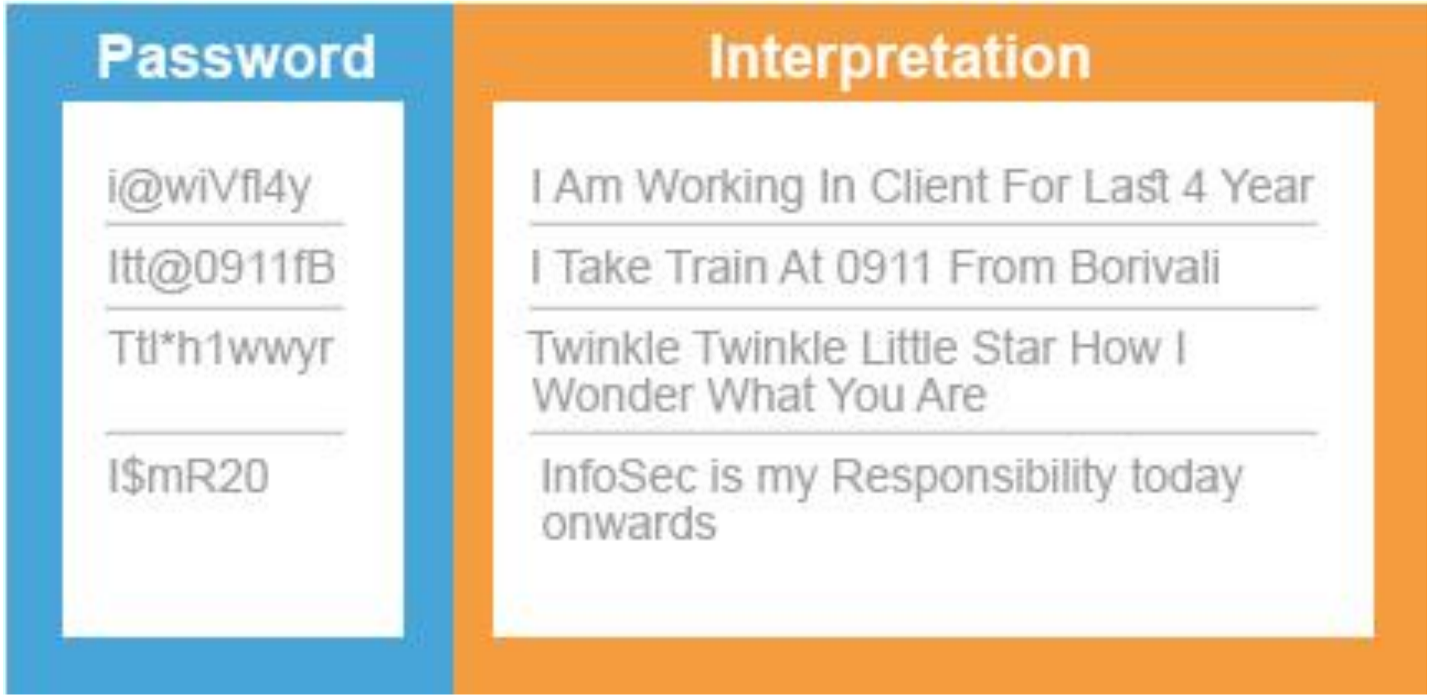
- Use strong passwords that meet the password criteria.
- Can be a known word or phrase converted using numerals, special characters.
- Should be difficult to guess for others but easy for you to remember.
- Change default passwords provided by IT on first log-on.
- Change your passwords at regular intervals and when you suspect any malicious activity.
- Avoid reusing or recycling old passwords.

- Do not use same password for official and commercial use or personal account.
- Do not share your user credentials and passwords with others.
- Do not include passwords in any automated log-on process.
- Do not write down your passwords or keep records of password and share it with your colleagues.
- Do not have dictionary words or names of family members as a part of your password.

© Datamatics Business Solutions Ltd. All rights reserved.

STRONG PASSWORD

- Passwords should be complex
- At least 8 characters
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Punctuation marks (!@#$%^&*()_+=-) etc.



Password	Interpretation
i@wiVfl4y	I Am Working In Client For Last 4 Year
Itt@0911fB	I Take Train At 0911 From Borivali
Ttl*h1wwyr	Twinkle Twinkle Little Star How I Wonder What You Are
I$mR20	InfoSec is my Responsibility today onwards

© Datamatics Business Solutions Ltd. All rights reserved.

EMAIL PROTECTION

- Use email for official purposes only.
- Follow the mail storage guidelines to avoid blocking of E-mails.
- If you come across any junk / spam mail, do the following:
  - Delete the mail immediately
  - Inform the IT Team

- Do not send or forward:
  - Any offensive or threatening material.
  - Unsolicited bulk mails (“spam” or “junk mail”).
- Do not share your email account password with anyone.
- Do not open attachments from unknown sources. Save and scan e-mail attachments for virus before opening them.
- Do not send business related information using external mail.
- Do not use email system to send chain letters, send messages containing inappropriate language.

© Datamatics Business Solutions Ltd. All rights reserved.

INTERNET ACCESS

- Use internet for business purpose only.
- Be cautious when entering sensitive information on web.
- Inform IT in case you come across any malicious sites.

- Download or Upload inappropriate or prohibited material such as music files, unlicensed software, freeware, video files, pornographic material, games or pictures for personal use.
- Post company information on any publicly accessible forums.
- Use internet for illegal activities such as gambling.
- Use Datamatics logos or materials on any web page or Internet posting unless it has been approved, in advance, by the management.

© Datamatics Business Solutions Ltd. All rights reserved.

INFORMATION BACKUP AND SECURITY

- Protect all sensitive information from disclosure to persons who do not have a need to know.
- Destroy removable media like CDs/DVDs, external HDDs, Pen drives using shredder before disposing (Take help from IT).
- Make sure that all your critical data is backed up.
- Follow Classification guidelines for your information assets.
- Shred your important documents before disposing them into the dustbin.

- Do not leave confidential documents unattended.
- Do not discuss sensitive information in public areas.

© Datamatics Business Solutions Ltd. All rights reserved.

INCIDENT MANAGEMENT

Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information and Information Systems of Client.

- Software malfunctions
- Information leakage
- Virus attack, Hacking
- Theft, Unsupervised visitor movement
- Tampering with restricted resources,
- Unauthorized access to IT infrastructure, premise, etc.
- Any violations of Datamatics's security policies and procedures shall also be considered an incident

© Datamatics Business Solutions Ltd. All rights reserved.

INCIDENT REPORTING

- Report incidents / exceptional situations to your managers and Premise Security officer.

- Escalate all the incidents as per the defined Incident Management policies & procedures.

- Do not try and test the weaknesses, since it might be interpreted as misuse of the system.

Incident Reporting

For any clarifications or in the event of an information security emergency, please contact your IS Management Team

© Datamatics Business Solutions Ltd. All rights reserved.

POTENTIAL DISCIPLINARY ACTIONS

Management Review

Strict action may be taken against users found to be in violation of organization’s Information Security Policies and Procedures. The punitive action may be decided on a case-to-case basis depending on the impact of the violation on the information systems resources.

Possible Punitive Actions would be:

- For High Severity - Suspension of Service / Termination of Employment / Cancellation of Contract.
- For Medium Severity - Severe Reprimand / Warning memo / Suspension of Service.
- For Low Severity – Reprimand.

© Datamatics Business Solutions Ltd. All rights reserved.

AUDIT CONCERNS

- What should we as employees be aware of?
  - Policies
  - Procedures
  - Basic Security requirements

- What can we do to ensure that the audit is smooth?
  - Our workspace is clean. No unwanted stuff lying around.

© Datamatics Business Solutions Ltd. All rights reserved.

VERSION CONTROL OF QMS AWARENESS PPT

Name of Doc : ISMS Awareness ppt
Doc Code : WI1003
Ver : 2.1
Ver Dt : 22-Feb-24
Classification : Internal
Prepared by : Compliance

© Datamatics Business Solutions Ltd. All rights reserved.

Datamatics
Business Solutions

THANK YOU

IND: +91 22 6771 2001

US: +1 571 281 0707

EU: +44 2030 265 330

EMAIL: marketing@datamaticsbpm.com

WEBSITE: www.datamaticsbpm.com