Information Security Awareness

hoonartek

An ISO 9001 QMS | ISO 27001 ISMS | ISO 22301 BCMS Certified Company

Table of Content

1. What is Information Security?
2. Importance of Information Security within an Organization
3. Threats towards Information Security of an Organization
4. Your Responsibility – Information Security

What is Information Security?

Information security refers to the practice of protecting information and data from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing policies, procedures, and technologies to ensure the confidentiality, integrity, and availability of information.

Information security aims to protect all forms of data, including electronic data stored on computers, networks, and other digital devices, as well as physical data such as paper documents and other tangible objects. It also involves protecting the systems and networks that process and store data, as well as the people who use them.

There are several components of information security, including:

- Confidentiality: Ensuring that only authorized individuals can access sensitive information.
- Integrity: Maintaining the accuracy and completeness of data and ensuring that it has not been tampered with or altered.
- Availability: Ensuring that information is accessible and usable by authorized users when needed.
- Authentication: Verifying the identity of individuals who access systems and data.
- Authorization: Granting access privileges to individuals based on their roles and responsibilities.
- Encryption: Converting data into a secret code to protect it from unauthorized access.
- Backup and recovery: Creating backups of data to prevent data loss in case of a security breach or system failure.

Importance of Information Security within an Organization

Information security is of paramount importance in today's digital age as organizations rely heavily on technology and data to conduct their business operations. Information security refers to the practice of protecting sensitive data and information from unauthorized access, use, disclosure, disruption, modification, or destruction.

Here are some reasons why information security is crucial:

- Protecting confidential data: Information security helps protect sensitive data such as trade secrets, financial records, and personal information from unauthorized access. Breaches of such data can have serious legal, financial, and reputational consequences.
- Maintaining business operations: Cyber attacks and security breaches can cause significant disruptions to business operations, leading to financial losses, reputational damage, and potential legal liability. By ensuring information security, businesses can prevent such disruptions and maintain business continuity.
- Complying with regulations: Many industries have regulations and laws that require companies to protect sensitive data. Information security helps companies comply with these regulations and avoid fines, legal liability, and damage to their reputation.
- Building trust with customers: Consumers and clients are increasingly concerned about the security of their personal information. By prioritizing information security, companies can build trust with their customers and strengthen their reputation.
- Staying ahead of cyber threats: Cyber threats are constantly evolving, and hackers are always looking for new vulnerabilities to exploit. Information security helps organizations stay ahead of these threats by implementing the latest security technologies and practices.

Threats towards Information Security of an Organization

There are many different threats to information security, and they can come from a variety of sources, including:

- Malware: This is software that is designed to harm or disrupt computer systems, steal data, or allow unauthorized access to sensitive information.
- Phishing: This is a type of social engineering attack where attackers use emails, phone calls, or other forms of communication to trick users into revealing sensitive information, such as login credentials.
- Password attacks: These attacks involve attempting to guess or crack passwords to gain access to a system or network.
- Insider threats: These are threats that come from individuals who have authorized access to a system, such as employees or contractors, who intentionally or accidentally leak sensitive information or cause other security breaches.
- Denial of service (DoS) attacks: These attacks involve overwhelming a network or system with traffic or requests, making it unavailable to legitimate users.
- Advanced persistent threats (APTs): These are targeted attacks that are typically carried out by skilled and well-funded attackers who seek to gain long-term access to a network or system in order to steal sensitive information.
- Physical theft or damage: This involves physically stealing or damaging hardware or other physical assets that contain sensitive information.
- Social engineering: This refers to a wide range of techniques that attackers use to manipulate people into divulging sensitive information or performing actions that are not in their best interest.

Your Responsibility – Information Security

1. Have designated Project operations areas with restricted accesses to unauthorized personnel.
2. Ensures awareness amongst project team members on information security policies followed at HoonarTek.
3. Show Zero tolerance to credentials and password sharing, saving any client data on private drives etc.
4. Discourage shoulder surfing while working on client data.
5. Implement and follow clean desk and clear desktop policy. Never leave any information unattended.
6. Never discuss important business matters of the organization in public areas, café, restaurants etc. where there is a high footfall of unknown people who may be exposed to sensitive information. Always use a soundproof discussion area where the information discussed will remain within the designated group of individuals.
7. As part of the best practice, always remember to lock your computer screen while moving away from your computer. This will ensure information on your computer is secured.
8. If you are unsure of the source of emails from external sources, never click on such emails or download any files attached to these emails. These files may be ransomware, malware or viruses which may affect and compromise the information security of the entire organization.
9. Be wary of unsolicited requests: If someone you don't know contacts you and asks for sensitive information, such as your password or financial details, be cautious. Verify their identity before sharing any information, and don't trust unsolicited requests.
10. Verify before trusting: Verify the identity of anyone who requests sensitive information or asks you to perform an action, such as clicking on a link or installing software. Use a trusted source of information, such as an official website or phone number, to confirm their identity.
11. Keep personal information private: Be careful about sharing personal information online or in public. This includes information such as your full name, date of birth, address, and phone number. Use privacy settings on social media and other online accounts to limit access to your information.
12. If you are unsure what is to be done if you feel there is a threat, seek assistance from the IT Helpdesk team immediately.

In case of Queries and Questions…..

You can reach out to us on – assurance@hoonartek.com

You can refer to policies for Information Security standards at HoonarTek at

https://hoonartek.keka.com/ui/#/org/documents/org

Please note that the ISMS Awareness Program will not be considered complete till the quiz is answered by you.

Link for ISMS Quiz - https://forms.office.com/r/F1Y8eijgW5

Thank You