ENG3004 - Individual Assignment 1

Student Name: KONG KWUN LAM Student Name: 22026839D

Answer:

Maintaining confidentiality is important because maintaining confidentiality helps build trust with clients, customers, and other stakeholders. When sensitive information is kept confidential, clients and customers are more likely to trust the company with their information and business. Also, it helps preserving competitive advantage. Confidential information, such as trade secrets, can give companies a competitive advantage by prevent competitors from accessing or using it. Moreover, many industries have strict regulations regarding the protection of confidential information. Companies must comply with these regulations to avoid legal and financial consequences. Last but not least, to protect company reputation. Confidential information breaches can result in significant negative publicity and damage a company's reputation. The company can ensure that privileged information is handled properly by the employees by implementing the following measures:

1. **Developing a strict confidentiality policy**:

Confidentiality policy refers to a set of guidelines or rules that dictate how sensitive information should be handled, stored, and protected. This policy establishes the responsibility of individuals to maintain the privacy of confidential information and prevent unauthorised access, use, or disclosure. Some common elements of a confidentiality policy include:

- Definition of confidential information, including the types of information that are considered confidential and the criteria for determining what is considered confidential
- Guidelines for handling confidential information, including how it should be stored, transmitted, and disposed of
- Responsibility of individuals and organisations to maintain confidentiality, including the consequences of unauthorised access, use or disclosure of confidential information
- Access controls and security measures to protect confidential information, including passwords, encryption, and firewalls.

The purpose of a confidentiality policy is to ensure that sensitive information is protected and to reduce the risk of unauthorised access, use, or disclosure. This policy helps to maintain trust and integrity, and it is essential for organisations to have in place to comply with legal and regulatory requirements.

2. Providing training:

Training employees to maintain confidentiality information is crucial for ensuring the protection of sensitive information and maintaining the trust of clients, customers, and other stakeholders. The following are steps that can be taken to effectively train employees on confidentiality:

- Clearly define what constitutes confidential information: Start by providing a clear definition of what information is considered confidential and what is not. This will help employees understand what information they are responsible for protecting.
- Explain the importance of confidentiality: Explain why maintaining confidentiality is important for the organization and its clients, customers, and stakeholders. Explain the potential consequences of a breach of confidentiality, including legal and financial implications.
- Provide written policies and procedures: Provide employees with a written policy that outlines the organisation's confidentiality policies and procedures. This policy should be regularly reviewed and updated as needed.
- Provide hands-on training: Provide hands-on training that demonstrates how to store, transmit, and dispose of confidential information. This can include training on the use of secure email, password protection, and encryption.
- Reinforce the importance of confidentiality: Regularly reinforce the importance of confidentiality and the consequences of a breach of confidentiality. This can be done through regular communications, training sessions, and reminders.
- Monitor and enforce the confidentiality policy: Regularly monitor the implementation of the confidentiality policy and enforce it when necessary. This includes taking appropriate action when a breach of confidentiality occurs.

Training employees to maintain confidentiality information is an ongoing process that requires regular reinforcement and monitoring. By providing clear policies, hands-on training, and regular reinforcement, organisations can ensure that employees understand the importance of confidentiality and take the necessary steps to protect sensitive information.

3. Using technology:

Technology plays a crucial role in maintaining confidentiality information, as it provides a range of tools and solutions to help organizations secure and protect sensitive information. Some of the ways technology can be used to maintain confidentiality information include:

- Encryption: Encryption is a process that converts plaintext into cipher-text,

making it unreadable to anyone without the decryption key. Encryption can be used to secure data in transit, such as when sending emails or transmitting data over the Internet, or to secure data at rest, such as when storing it on a hard drive or cloud storage service.

- Access control: Access control systems are used to manage and control access to confidential information. This includes setting up user accounts and permissions, setting up firewalls and intrusion detection systems, and monitoring access to confidential information.
- Data backup and disaster recovery: Data backup and disaster recovery systems are used to ensure that confidential information is protected in the event of a disaster, such as a fire, flood, or cyber attack. This includes regularly backing up data to secure offsite locations and having a disaster recovery plan in place to ensure that confidential information can be quickly and easily restored in the event of a disaster.
- Mobile device management: This solutions are used to manage and secure mobile devices, such as smartphones and tablets, that are used to access confidential information. This includes setting up encryption, password protection, and remote wipe capabilities, and monitoring access to confidential information on mobile devices.

By using technology to maintain confidentiality information, organisations can ensure that sensitive information is protected and secure, and that confidential information remains confidential. Conducting background checks: The company should conduct background checks and verify the employment history of new hires to ensure that they have a track record of maintaining confidentiality.

4. Implementing physical security measures:

The company should secure physical access to confidential information by implementing measures such as locked file cabinets, password-protected computers, and secure printing and scanning procedures. Some of the physical security measures that can be used to protect confidential information include:

- Controlled access: Controlled access involves limiting the number of people who have access to confidential information and ensuring that access is granted only to those who need it. This can be achieved through the use of security passes, keycard access systems, or other physical security measures.
- Secure storage: Secure storage involves storing confidential information in a secure location, such as a locked cabinet or a secure room, to prevent unauthorised access.
- Document destruction: Document destruction is the process of destroying

confidential information that is no longer needed. This can be done through shredding, burning, or other methods to ensure that the information cannot be recovered.

- Video surveillance: Video surveillance can be used to monitor access to confidential information and detect unauthorised access attempts.
- Physical barriers: Physical barriers, such as locked doors, walls, or partitions, can be used to prevent unauthorised access to confidential information.

By implementing these and other physical security measures, organisations can help ensure the confidentiality of sensitive information and prevent unauthorised access, use, or disclosure.

5. Taking legal action:

Legal action can be used to maintain information confidentiality and prevent unauthorised access, use, or disclosure of confidential information. Some of the legal measures that can be used include:

- Non-disclosure agreements (NDAs): NDAs are legal contracts that prohibit the recipient of confidential information from disclosing it to others. NDAs can be used to protect confidential information shared between individuals or organisations.
- Trade secret protection: Trade secret protection is a legal mechanism that allows organisations to protect confidential information that gives them a competitive advantage. Organisations can use trade secret protection to prevent competitors from accessing or using their confidential information.
- Copyright protection: Copyright protection can be used to protect confidential information that is original and fixed in a tangible form, such as a document or software code.
- Litigation: Litigation is the process of taking legal action in a court of law. Organisations can use litigation to seek remedies for breaches of confidentiality, such as injunctions, monetary damages, or other legal remedies.

By using these and other legal measures, organisations can help protect their confidential information and prevent unauthorised access, use, or disclosure.

Reference:

1. *10 best cyber security technology trends you must know*. HKR Training. (n.d.). Retrieved February 16, 2023, from https://hkrtrainings.com/cyber-security-technologies

2. Bika, N. (2022, July 25). *Employee confidentiality policy*. Recruiting Resources: How to Recruit and Hire Better. Retrieved February 16, 2023, from https://resources.workable.com/confidentiality-company-policy
3. *How to protect Workplace Confidential Information: Blue-Pencil*. Blue. (n.d.). Retrieved February 16, 2023, from https://www.blue-pencil.ca/how-do-you-protect-confidential-information-in-the-workplace/
4. *The law on protection of confidential information*. (n.d.). Retrieved February 16, 2023, from https://www.wto.org/english/thewto_e/acc_e/cgr_e/WTACCCGR24A2_LEG_11.pdf