ENG3004 - Individual Assignment 1

Name NG TAI LOI

Student number 22032496d

Date 16 Feb 2023

Number of words 625

To begin with, the company must establish clear policies and procedures that define the types of information that must remain confidential, and the consequences of mishandling such information. To ensure that confidential information is handled properly by employees, companies can implement various measures. One of these is data classification, which involves establishing a system for classifying data based on its sensitivity to ensure that appropriate security controls are implemented. This can be done by assigning a classification label to each piece of information, based on its level of confidentiality. Information that is classified as "highly confidential" should be subject to more stringent security measures, such as encryption or limited access, than information that is classified as "moderately confidential" (Parker, 2020).

In addition to data classification, regular employee training and awareness campaigns are also essential in reinforcing the importance of confidentiality. Employees should be educated on the risks associated with mishandling confidential information and the consequences of breaching confidentiality. This can be done through online training modules, in-person training sessions, or regular company-wide awareness campaigns. These policies must be effectively communicated to all employees to ensure their understanding and compliance. Additionally, regular training and education must be provided to employees to keep them up-to-date with best practices for data handling and safeguarding.

Access to confidential information should be restricted to only those employees who require it to perform their job functions. Non-disclosure agreements may also be used to legally bind employees to confidentiality obligations. Furthermore, the company could consider implementing physical and digital security measures to augment the security of confidential information. Physical security measures might include access-controlled rooms, locking file cabinets, and biometric or multi-factor authentication, while data security measures could include encryption of data at rest and in transit, firewalls, intrusion detection systems, and antivirus software.

To further ensure that confidential information is handled properly by employees, the company could also consider implementing access controls based on role-based access or access management software, data classification systems based on the sensitivity of the information, regular employee training and awareness campaigns, and physical security measures such as secure storage facilities and security cameras. A clear incident response plan should also be established to outline the steps to be taken in the event of a data breach.

In addition, the company should adopt effective hiring practices, such as conducting background checks on prospective employees, verifying their previous employment history, and reviewing references. Employment contracts should also include clauses on confidentiality, non-disclosure, and non-compete obligations to reinforce the importance of protecting confidential information.

In the event of a data breach, the company should have a well-defined plan in place to manage the situation, including incident response procedures and a communication plan with affected parties. By implementing these measures, the company can take a proactive approach to managing the risks associated with handling confidential information and protect its most valuable assets. A clear incident response plan should also be established to outline the steps to be taken in the event of a data breach. The plan should include procedures for containing the breach, identifying the source of the breach, and notifying affected parties. This plan should be regularly reviewed and updated to ensure that it remains current and effective.

In conclusion, ensuring the proper handling of privileged information by employees is crucial for protecting a company's most valuable assets. By implementing a combination of policies and procedures, employee training and education, access controls, security measures, effective hiring practices, and incident response planning, a company can minimize the risk of a breach and ensure the confidentiality of its information. By implementing these additional measures, a company can further reduce the risk of a breach of confidential information and ensure that its most valuable assets are protected.

References

2022 top priorities for Legal & Compliance. Gartner. (n.d.). Retrieved February 13, 2023, from https://www.gartner.com/en/legal-compliance/trends/top-priorities-legal

NIST SP 800-171. (n.d.). Retrieved February 13, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Workplace Privacy and employee monitoring. PrivacyRights.org. (n.d.). Retrieved February 13, 2023, from https://privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring

Internet protocol event reporting - security industry association. (n.d.). Retrieved February 14, 2023, from https://www.securityindustry.org/wp-content/uploads/2017/10/dc09_r2021_20201027.pdf