Q1) Company’s most valuable assets is information. Employees are supposed to maintain the confidentiality of information (whether or not it is considered proprietary) entrusted to them not only by the Company, but also by suppliers, customers and others related to the business. If disclosed, might be of use to competitors or harmful to the Company, or its customers or suppliers. With reference to the above, recommend how the company can make certain that the privileged information is handled properly by the employee?

According to the dictionary of Cambridge, privileged information is secret information that is legally protected so that it does not have to be given to the public: Companies should explicitly decide what is privileged information and set up strict protocols for who has access to it.

Companies can ensure that employees properly handle privileged information by.

First of all, companies can implement proper access controls for employees.

1) Companies can establish the risk exposure and sensitivity of information or data, and divide them into different security levels, and employees need to regularly review whether the security level of information or data is appropriate.

2) The company can restrict employees' access to or browse privileged information or sensitive materials and avoid idlers from viewing them. The company can only approve employees' access or browsing based on the actual application of the principles of need-to-know, need-to-do and need-to-use.

3) Companies can set and use passwords to restrict employees from accessing or viewing sensitive information, and passwords should be changed regularly to prevent theft.

4) Companies establish audit trails for computer systems to identify those who have gained access to information to facilitate investigations and access control monitoring.

Second, companies can monitor information releases.

1) Companies can provide clear guidelines for employees to learn how to safely hold and handle the release of confidential information and how to protect computer security through employee training.

2) The company can monitor how employees release information according to the principle of need to know, need to do, and need to use.

3) Employees can only disclose confidential information related to them after obtaining authorization from their employers and customers.

In addition, the company ensures appropriate information management controls.

1) The company needs to clearly communicate the company's confidentiality policy to employees at all levels. And such policies are regularly reviewed to assess their effectiveness in minimizing risks.

2) The company should establish principles to remind employees of the serious consequences of leaking or abusing proprietary information and avoid leaks or abuse.

3) The company may require employees to sign an agreement not to disclose or misuse proprietary information during their tenure and for a specified period after leaving the company. Otherwise, the employee can be prosecuted according to the regulations in the agreement.

And companies can advise employees to use confidential waste bins and paper shredders. When employees need to dispose of sensitive documents, be sure to shred them or use a confidential trash can. Issues like identity theft mean you should never assume that because a file is in the Trash, no one else will look at it.

Also, Employees can use lockable file storage cabinets to store confidential documents. If an employee leaves the company, unattended files can be placed in a storage cabinet to prevent others from taking them.

I believe the above methods can effectively help companies how to ensure that employees properly handle privileged information.

Reference:

https://blog.grantmcgregor.co.uk/2017/5-top-tips-for-handling-confidential-information-in-your-business

ethics in practice
ETHICS_IN_PRACTICE.pdf