To ensure that employees appropriately handle privileged information, the company needs to implement proper access control, monitor the release of information, and ensure proper management controls.

Access Control:
The first step in safeguarding privileged information is to classify information into different security groups based on risk exposure and sensitivity. This classification should be reviewed regularly to ensure that information is appropriately classified. Based on the classification, the company should approve access rights based on the need-to-know, need-to-do, and need-to-use principles. This means that only those employees who have a genuine need to use the information during their duty can have access to classified information. The company should also restrict access to computer information by using passwords and ensuring that passwords are changed regularly. An audit trail system for computer systems should be set up to identify persons who have gained access to information to facilitate future investigations and access control monitoring.

Monitoring Release of Information:
The company should provide clear guidelines on how to safeguard and handle the release of classified information and how to ensure computer security. These guidelines should be reviewed regularly to ensure they remain relevant and effective in minimizing risk. Monitoring of the release of information should be conducted according to the need-to-know, need-to-do, and need-to-use principles. Before disclosing confidential information to an employer or client, the company should obtain authorization. This helps to ensure that information is not released to unauthorized persons.

Proper Management Controls:
The company should clearly communicate its policy on the preservation of confidentiality to all levels of staff. The policy should be reviewed regularly to assess its effectiveness in minimizing risk. Employees should be made aware of the severe consequences of leaking or abusing proprietary information. To ensure that employees understand the seriousness of the issue, the company should require employees to sign agreements not to leak or misuse proprietary information during their employment and for a specific period after they have left the company if necessary.

In addition to these measures, the company can also provide regular training to employees on the importance of safeguarding privileged information and the consequences of failing to do so. The company should also conduct regular assessments to identify potential vulnerabilities in its systems and processes that could result in the unauthorized disclosure of information.

Overall, implementing these measures can help the company ensure that privileged information is handled properly by its employees, reducing the risk of unauthorized disclosure and protecting the company's valuable assets.