Task 1:

Trong xây dựng thương mại và dân dụng, tường lửa là tường xây bằng bê tông hoặc tường được xây chạy từ tầng hầm qua tới mái nhà để ngăn đám cháy lan từ vị trí này sang vị trí khác của toà nhà. Trong máy bay và ô tô, tường lửa là một hàng rào kim loại cách nhiệt giúp giữ các bộ phận nóng và nguy hiểm của động cơ chuyển động tách biệt với phần bên trong dễ cháy nơi hành khách ngồi. Tường lửa trong chương trình bảo mật thông tin tương tự như tường lửa của một tòa nhà ở chỗ nó ngăn các loại thông tin cụ thể trôi nổi bên ngoài, được gọi là mạng không đáng tin cậy (ví dụ: Internet) và bên trong, được gọi là mạng đáng tin cậy. Tường lửa có thể là một hệ thống máy tính riêng biệt, một dịch vụ với 63 phần mềm chạy trên bộ định tuyến hoặc máy chủ hiện có, hoặc một mạng riêng có chứa một số thiết bị hỗ trợ. Trong tin học, tường lửa là một hệ thống an ninh mạng giám sát và kiểm soát lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật được xác định trước. Tường lửa thường thiết lập một rào cản giữa mạng nội bộ đáng tin cậy và mạng bên ngoài không đáng tin cậy, chẳng hạn như Internet. Tường lửa có thể được phân loại theo cách thức xử lý, thời kỳ phát triển hoặc cấu trúc. Thuật ngữ tường lửa ban đầu dùng để chỉ một bức tường nhằm mục đích giới hạn ngọn lửa trong một dãy các tòa nhà liền kề. Các sử dụng sau này đề cập đến các cấu trúc tương tự, chẳng hạn như tấm kim loại ngăn cách khoang động cơ của xe hơi hoặc máy bay với khoang hành khách. Thuật ngữ này được áp dụng vào cuối những năm 1980 cho công nghệ mạng, xuất hiện khi khả năng sử dụng, kết nối toàn cầu của Internet còn khá mới. Tiền thân của tường lửa để bảo mật mạng là các bộ định tuyến được sử dụng vào cuối những năm 1980, vì chúng phân tách các mạng với nhau, do đó ngăn chặn sự lây lan của các vấn đề từ mạng này sang mạng khác. Trước khi nó được sử dụng trong máy tính đời thực, thuật ngữ này đã xuất hiện trong bộ phim về hack máy tính WarGames năm 1983, và có thể là nguồn cảm hứng cho việc sử dụng nó sau này.

Task 2:

Employees are the greatest threats since they are the closest to the organizational data and will have access by nature of their assignments. They are the ones who use it in everyday activities, and employee mistakes represent a very serious threat to the confidentiality, integrity, and availability of data. Employee mistakes can easily lead to the revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information.

By employing the following practices and solutions, we can prevent it:

Update corporate security policy. Security policy should clearly outline how to handle critical data and passwords, who can access them, which security and monitoring software to use, etc. Revise security rules and check whether all current best practices are reflected in the document.

Educate employees. Make employees aware of potential threats and explain how dangerous and expensive the consequences of their mistakes can be. We should educate our employees about risks such errors pose to the organization’s security. Make sure everyone is familiar with the corporate security policy and is motivated to follow the rules.

Use the principle of least privilege. The easiest and most reliable way to secure data access is to deny all access by default. Allow privileged access only when needed on a case-by-case basis. If users

can only access data required for their work, we can prevent accidental data leaks and data deletion caused by employees who aren't supposed to work with certain sensitive data in the first place.

Monitor employees. User activity monitoring tools are needed to detect malicious activity and secure system from data leaks and malicious attacks. The most reliable way to ensure accurate detection and prevention of security mistakes is by using employee monitoring software such as Ekran System.