**1. Trách nhiệm công việc chung cho vị trí Giám đốc bảo mật thông tin**

1. Chịu trách nhiệm đảm bảo các chiến lược quản trị và sự liên kết với an ninh vật lý được phù hợp với mục tiêu kinh doanh của tổ chức. (Nghĩa là tăng trưởng / Sáng tạo, hiệu quả hoạt động, đáng tin cậy, quản lý rủi ro và Tuân thủ quy định).
2. Chỉ đạo nhân viên IT cấp dưới trong việc xác định, phát triển, thực hiện và duy trì các quá trình toàn tổ chức để giảm rủi ro dữ liệu và toàn hệ thống công nghệ thông tin. Đảm bảo sự liên kết giữa các nhóm công nghệ và đội ngũ lãnh đạo kinh doanh liên quan đến mối đe dọa, mức độ rủi ro, dữ liệu và các công nghệ bảo mật.
3. Thiết lập và duy trì tổ chức tiêu chuẩn công nghệ bảo mật, cải tiến quy trình, quy trình quản trị và số liệu hiệu suất để đảm bảo rằng mọi người, quy trình và công nghệ giảm thiểu các mối đe dọa liên tục và đáp ứng (NERC) tiêu chuẩn đáng tin cậy thông qua các tổ chức và bảo vệ công ty của tài sản thông tin.
4. Xác định, lựa chọn và thực hiện các tiêu chuẩn công nghệ bảo mật mà bổ sung cho tiêu chuẩn (như NIST, IS27001, COBIT).
5. Phát triển một chương trình phục hồi thực tế thảm họa tốt nhất để đảm bảo tính sẵn sàng công nghệ và an toàn cho hoạt động kinh doanh.
6. Thiết lập và quản lý quy trình cho các chiến lược giám sát an ninh mạng, các chính sách, kiểm soát tuân thủ, và các chương trình để đáp ứng nhu cầu kinh doanh của công ty.
7. Xác định nhu cầu và rủi ro an ninh thông tin, và lập kế hoạch hoạt động cho phù hợp với tầm nhìn, sứ mệnh và mục tiêu, và hỗ trợ tăng trưởng dài hạn Bảo mật thông tin và tính bền vững của tổ chức .
8. Hiểu, giao tiếp, thực hiện nhiệm vụ, huấn luyện và cố vấn cho các đội quản lý thông tin an ninh để phát triển kỹ năng, khả năng làm việc theo nhóm và toàn tổ chức công nghệ.
9. Giám sát việc lựa chọn, phát triển, triển khai, giám sát, bảo trì và tăng cường các tổ chức công nghệ an ninh mạng. Việc đánh giá trực tiếp của rủi ro kinh doanh và công nghệ để đảm bảo rủi ro đó được xác định một cách thích hợp và đánh giá. Giám sát việc phát triển và thực hiện các biện pháp thích hợp để xác định các rủi ro liên quan đến các chức năng ứng dụng / kinh doanh.
10. Cung cấp việc giám sát quản lý cho tất cả các hoạt động liên quan đến việc tuân thủ công nghệ với các quy định cũng như các yêu cầu kiểm toán, đảm bảo rằng công nghệ thực hành tốt nhất đang được theo dõi trong bảo mật thông tin và khôi phục thảm họa.
11. Cung cấp giám sát để phát triển, thực hiện và quản lý các chương trình khôi phục thảm họa công nghệ doanh nghiệp để đảm bảo kịp thời phục hồi hoạt động công nghệ sau gián đoạn dịch vụ do mất điện hệ thống công nghệ hay thảm họa khai báo.
12. Xây dựng chiến lược truyền thông để thông báo cho nhân viên của các sáng kiến an ninh mạng.
13. Phát triển kế hoạch nguồn lực để giải quyết các mối đe dọa mạng trong tương lai và các sáng kiến chiến lược trong tương lai.
14. Liên tục tìm kiếm và xem xét các giải pháp sáng tạo cho các vấn đề kinh doanh và áp dụng có liên quan trong việc hỗ trợ sứ mệnh của tổ chức.
15. Xây dựng và duy trì mối quan hệ hiệu quả thông qua Cơ quan giữa các chức năng khác nhau và các đơn vị kinh doanh để hỗ trợ các mục tiêu kinh doanh.
16. Quản lý nhân viên IT, bao gồm cả quản lý hiệu quả, quản lý tiền lương, và cân bằng khối lượng công việc.

**2. Kỹ năng thông thường cho một vị trí Giám đốc bảo mật thông tin**

1. Kiến thức về kiến trúc doanh nghiệp và rủi ro Quản trị và tuân thủ (GRC).
2. Quản lý chương trình và dự án, báo cáo rủi ro và thành lập các chỉ số rủi ro chính và các chỉ số hiệu suất chính
3. Thông tin công nghệ bảo mật, thị trường và các nhà cung cấp bao gồm tường lửa, phát hiện xâm nhập, các công cụ đánh giá, mã hóa, tổ chức chứng nhận, trang web, và phát triển ứng dụng.
4. Có khả năng xây dựng chiến lược, lộ trình và đầu tư.
5. Có kinh nghiệm xây dựng cơ cấu tổ chức và trách nhiệm.
6. Kỹ năng quản lý mối quan hệ nội bộ, hội đồng quản trị, thực thi pháp luật và kiểm toán.
7. Kiểm toán và đánh giá các phương pháp, thủ tục và thực hành tốt nhất có liên quan đến thông tin mạng, các hệ thống và các ứng dụng, hệ thống an ninh ứng dụng, công nghệ cơ sở dữ liệu dùng để lưu trữ thông tin doanh nghiệp, dịch vụ thư mục, thông tin tài chính và thông tin kiểm toán hiểu biết mạnh mẽ như thế nào để áp dụng công nghệ bảo mật hiện tại và đang nổi lên để giải quyết vấn đề kinh doanh.
8. Kỹ năng lập hồ sơ theo dõi của việc phát triển và triển khai ứng phó và phục hồi các chiến lược toàn diện, kế hoạch và thủ tục. sự hiểu biết toàn diện về thực hành và các luật liên quan đến dữ liệu riêng tư và bảo vệ.
9. Kỹ năng giao tiếp bằng lời nói và bằng văn bản, đặc biệt là trong lĩnh vực trình bày thuyết trình và tương tác với những người ở tất cả các cấp trong toàn tổ chức.
10. Lập hồ sơ theo dõi việc quản lý thành công của các chương trình và con người, cả bên trong và bên ngoài, cũng như kỹ năng chương trình / dự án / quản lý nhà cung cấp phức tạp chứng minh.
11. Nhanh nhẹn, linh hoạt, linh hoạt và khả năng làm việc với liên tục thay đổi các ưu tiên.

**3. Yêu cầu chung cho một vị trí Giám đốc bảo mật thông tin**

1. Cử nhân Khoa học Bằng cấp Kỹ thuật Công nghệ, Khoa học máy tính, hoặc tương đương.
2. 10 năm kinh nghiệm lãnh đạo tiến bộ trong bảo mật máy tính và thông tin, trong đó có kinh nghiệm với công nghệ Internet và các vấn đề an ninh.
3. Cấp giấy chứng nhận chính thức trong quản lý thông tin an ninh: CompTIA Security +, CISSP, CISM, CISA, và / hoặc CEH một lợi thế.
4. Kinh nghiệm an ninh mạng trong ngành công nghiệp IT