4. Authority and access control policy Hierarchical pattern—a senior manager may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee. The policy should outline the level of authority over data and IT systems for each organizational role. Network security policy—users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts. 5. Data classification The policy should classify data into categories, which may include “top secret”, “secret”, “confidential” and “public”. Your objective in classifying data is: To ensure that sensitive data cannot be accessed by individuals with lower clearance levels. To protect highly important data, and avoid needless security measures for unimportant data. 6. Data support and operations Data protection regulations—systems that store personal data, or other sensitive data, must be protected according to organizational standards, best practices, industry compliance standards and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection. Data backup—encrypt data backup according to industry best practices. Securely store backup media, or move backup to secure cloud storage. Movement of data—only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network. 7. Security awareness and behavior Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification. Social engineering—place a special emphasis on the dangers of social engineering attacks (such as phishing emails). Make employees responsible for noticing, preventing and reporting such attacks. Clean desk policy—secure laptops with a cable lock. Shred documents that are no longer needed. Keep printer areas clean so documents do not fall into the wrong hands. Acceptable Internet usage policy—define how the Internet should be restricted. Do you allow YouTube, social media websites, etc.? Block unwanted websites using a proxy. 8. Responsibilities, rights, and duties of personnel Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.