# Cyber Security-Edge Program

|  |
| --- |
| Name: Afrin Faria  ID: 2111270  Batch: B11 |

|  |
| --- |
| Overview  A security policy is a large document that’s made up of many subdocuments and defines the  company’s security strategy.  It is a document that defines all the rules in the organization that all personnel need to  follow—including users, network administrators, security professionals, and the management team.  It is important to note that even the security team in the organization must follow the security policy  defined by the organization.  It should be stressed that the security policy is designed to protect the assets of the organization and  ensure that actions within the organization are legal and compliant with any regulations governing the  organization.  As mentioned, the security policy is made up of many subdocuments, with each subdocument covering  a specific area of concern, known as a policy.  These policies specify the dos and don’ts that everyone within the organization must follow.  The policies are created by the security professional but are sponsored by upper-level management.  The first step to creating a security policy is to get the support and approval of upper-level  management, to ensure that the policy will be enforceable  #  Structure of a Policy  The following sections should be part of any security policy:  ■ Overview:  This first section should identify what the purpose of the policy is and how it helps secure  the environment.  For example, the overview of the password policy should specify the need to have strong  passwords and secure usage of passwords.  ■ Scope:  The Scope section of the policy defines who the policy applies to.  For example, you should explicitly specify whether the policy applies to all employees,  contractors, and/or temporary employees.  You should also specify if the policy is to apply to all equipment within the organization.  ■ Policy:  The Policy section is the largest section in the document and is the listing of do’s and don’ts.  The policy section may be divided into different parts to help organize all of the rules  specified by the policy.  #  Structure of a Policy (Cont…)  ■ Enforcement:  A very important part of the policy is to specify what happens if employees  do not follow it.  The Enforcement section is usually a short section specifying that if  employees do not adhere to the policy, disciplinary action and maybe even  termination of employment could result.  ■ Definitions:  The Definitions section is where you can add definitions for terms that are used  in the policy that the reader of the policy may not know.  ■ Revision History:  The Revision History section of the policy lists the date the policy was  changed, who made the change, and maybe who authorized the change.  Do not forget to add an entry to the revision history showing the creation date  of the policy  #  Identifying types of Policies  Three popular types of policies are standards, guidelines, and procedures.  Standard:  Most policies within an organization are standards that must be followed.  A standard policy is a policy that needs to be followed and typically covers a specific area of security.  Failure to follow a standard policy typically results in disciplinary action such as termination of  employment.  Guidelines:  Some policies are guidelines, which are recommendations on how to follow security best practices.  In the past, the National Security Agency (NSA) had published on its web site a number of guidelines  on security best practices for different types of servers and operating systems.  No disciplinary actions result from not following a recommended policy because it is just that—a  recommendation.  Procedure  The final type of policy is a procedure policy, also known as a standard operating procedure (SOP).  The SOP documents step-by-step procedures showing how to configure a system or device, or  step-by-step instructions on how to implement a specific security solution.  #  General Security Policies  #  Overview  All organizations need a security policy as a starting point to implementing security  because the security policy defines the rules in the business and all the do’s and  don’ts.  Without the security policy in place, the security team has no idea what kind of  security controls to implement.  For example, the security policy will have a firewall policy that determines what  firewall products are used by the organization and what type of firewall rules are to  be applied. Without this policy, the firewall administrator will not know what to  configure on the firewall.  The term security control is used to identify any mechanism used to protect an  asset within the organization. Examples of security controls are firewalls, antivirus  software, and access control lists.  This section is designed to give you an idea of some of the different security policies  that should exist within your organization.  #  Policies affecting Users  The policies may affect how users interact with the assets within the  business on a daily basis.  Two popular policies that affect users are the acceptable use  policy and the password policy.  Acceptable Use Policy:  The acceptable use policy, also known as the AUP, is an important policy  because it lets the users know what the company considers acceptable use  of its assets such as Internet service, e-mail, laptops, and mobile devices.  Be sure to have all employees read and sign the acceptable use policy  to ensure that they understand what is considered acceptable use of  company assets such as computers, Internet service, and e-mail.  The acceptable use policy should be reviewed by all employees during  employee orientation and should be signed as proof that they have read the  policy and agree to its terms.  #  Policies affecting Users (Acceptable Use  Policies) (Cont…)  The following are topics typically covered by the acceptable use policy:  ■ Acceptable use of Internet :  Typically covers rules such as prohibiting inappropriate content.  You may also want to state whether the Internet should be used only for business purposes and what  the company tolerance is for use of social networking sites during business hours.  ■ Acceptable use of e-mail:  This policy should cover the fact that e-mail is for business use, with minimal personal e-mail allowed.  Also specify in the policy what the company rules are surrounding the topic of forwarding chain letters,  and specify that harassing e-mails cannot be sent from business e-mail accounts.  ■ Acceptable use of laptops:  This policy specifies any rules surrounding the use of laptops.  You may want to cover topics such as locking the laptop in the trunk if it is left in a car—laptops are  not to be left in plain view.  Also specify whether the content on the laptop should be encrypted and whether the user can connect  the laptop to non-work networks.  #  Policies affecting Users (Acceptable Use  Policies) (Cont…)  ■ Acceptable use of mobile devices:  This policy should cover any rules surrounding mobile devices, such as the types of  mobile devices that can be used for corporate e-mail and phone calls.  Also specify how much personal use is allowed with the mobile device and what to  do if the mobile device is stolen.  Lastly, you may want to specify what features of a mobile device are to be enabled  or disabled.  ■ Acceptable use of social media:  This policy should cover rules surrounding the use of social media and what type of  content the employee is allowed or not allowed to share or comment on.  For example, a company may specify that the employee is not to comment on  behalf of the company or give the impression that their viewpoints are those of the  company.  A different approach companies may take is that if an employee comments on a  product related to their industry, the employee must state that they work for the  company  #  Password Policy  The password policy is an important policy to both users and administrators.  The following outlines some of the considerations that should go into the password policy:  ■ Minimum password length:  The minimum password length specifies how many characters employees must have in their  passwords.  The typical minimum length used by businesses is eight characters.  ■ Password history  The password history setting specifies how many past passwords the system should keep track of.  The concept here is that employees are not allowed to reuse a password in the password history.  Companies typically set the history to 12 or 24 passwords.  ■ Maximum password age:  The maximum password age specifies how long an employee is allowed to have a specific password.  This value is normally set anywhere from 30 to 60 days, at which time the user must change their  password.  #  Password Policy (Cont…)  ■ Minimum password age  The minimum password age is a minimum number of days that a user must  have their password.  This setting prevents employees from changing their password multiple  times in order to get the desired password out of the history with the intent of  reusing an old password.  ■ Password complexity:  The password complexity setting specifies whether you require complex  passwords.  A complex password is one that has a mix of letters, numbers, and symbols  and uses a mix of uppercase and lowercase characters.  It is highly recommended to have password complexity enabled within your  environment.  #  Policies Affecting Personnel Management  The following policies should be defined to ensure the company knows what  actions to take when hiring a new employee or an employee leaves the  company:  ■ Nondisclosure agreement (NDA) :  The nondisclosure agreement should be read and signed by employees,  contractors, and management personnel to acknowledge that they understand and  accept that they cannot share sensitive information about the company that they  gain access to while working at the company.  The NDA applies not only while working for the company but also after the work  engagement has completed.  ■ Onboarding:  The company should have onboarding policies defined that specify for each job role  any specific training employees should have to help them in that job role.  This includes onboarding for employees, management, and executives.  Onboarding would also include granting access to resources such as a mobile  device.  #  Policies Affecting Personnel  Management(Cont..)  ■ Offboarding:  Offboarding policies would indicate procedures that should be taken when an employee leaves a  department or company.  For example, one of the procedures would be for the collecting of resources such as PKI cards and  company devices.  ■ Continuing education:  Training is one of those company perks that really help boost employee morale.  The company should have a continuing education policy defined that specifies each employee’s  budget for training per year based on their job role.  ■ Acceptable use policy/rules of behavior:  As previously described, the acceptable use policy defines the rules for how employees,  management, and executives are to use technologies such as mobile devices, e-mail, the Internet,  and social media.  ■ Adverse actions:  With the support of the executive team, each policy should specify adverse actions for anyone who  does not follow the security policies.  For example, employees should be put on notice that they could lose their job as a result of not  complying with the policy.  #  Policies Affecting Administrators  This section outlines some popular policies that should be in  place to guide the administrators to follow best practices.  Asset Management:  Organizations should have asset management policies; this includes  policies surrounding the purchasing, day-to-day management, and the  retiring of company assets.  For example, companies should have established suppliers that can  be contacted when new server hardware needs to be purchased.  There should be policies in place dictating the maintenance of the  server asset and how the asset is decommissioned once it has  exceeded its lifetime.  #  Policies Affecting Administrators(Cont…)  Change Control/Management Policy:  One of the most critical policies to have in place is a change control or  change management policy that specifies the process to follow when  implementing a change to the network.  When a change management process is not in place and the policy is  not being followed, access to the network may be denied due to  mistakes made when implementing changes.  Having a change management policy that specifies procedures to  follow should reduce mistakes in configuration because a process can  ensure that the change will be properly tested.  The change management policy should also specify who should be  notified of a change before it is implemented so that person can sign off  on the change.  #  Policies Affecting Administrators(Cont…)  Secure Disposal of Equipment Policy:  One of the most vital policies to consider today covers secure disposal of  equipment.  What do you do with a computer that has been decommissioned in the business?  Do you donate it to the local school system? What about the corporate data that  resides on the hard drive of that system?  It is important to have a policy that specifies what to do with systems and devices  after they are taken out of production.  In highly secure environments, it is critical that you physically destroy any hard  drives that hold sensitive data.  In less secure environments, you may want to securely wipe the drives so that the  data cannot be recovered.  Simply reformatting a drive does not remove the information, and it still can be  retrieved.  Also specify in the secure disposal of equipment policy what to do with other old  equipment taken out of production. This includes servers, tapes, switches, routers,  and mobile devices.  #  Policies Affecting Management  Although most policies directly affect the administrative team by  informing them how to make changes or what types of changes  need to be made, some policies directly affect management. This  section outlines a few policies that management should consider  to help protect their business and assets.  Privacy Policy  An important aspect to any organization today is to have a privacy  policy in place that is used to educate employees and customers as to  how and why information is collected from its customers and how that  information will be used.  Most businesses place a privacy statement on their web site to inform  the public how they intend to use and manage that information.  #  Policies Affecting Management(Cont..)  Information Classification Policies:  Another example of a policy that deals with the concerns of management is an information classification policy.  The information classification policy helps define the different classifications of information (for example, secret  and top secret) and what clearance level is needed to access that information.  Assigning a classification level (known as a data label) to information determines which security controls are used  to secure the information and how much money is invested in protecting that information.  The following are some popular information classifications used by the military:  ■ Top secret:  This is the highest classification level. Public disclosure of top secret information would cause grave damage to  national security.  ■ Secret:  A classification level below top secret. Public disclosure of information classified as secret could cause serious  damage to national security.  ■ Confidential:  A classification level below secret and the lowest classification level. Public disclosure of information classified as  confidential could cause damage to national security.  ■ Unclassified:  Any information that is not classified falls into this category. Public disclosure of unclassified information is  considered safe and not harmful to national security.  #  Policies Affecting Management(Cont..)  The security policy should specify what type of information is top secret, secret, confidential,  and unclassified.  The policy should specify not only how information is classified but also under what  circumstances information can be declassified (the classification removed or changed) and  what the process is to have that classification on the information changed.  Once the information in the organization has been classified, the next step is to assign to  persons within the organization a clearance level.  To access top secret information, for example, an employee would need top secret  clearance and need-to-know status.  Security Clearance and Data Labels:  Many people confuse the concepts of data classification labels and security clearance levels.  The classification labels (such as secret, top secret, or even unclassified) are assigned to the  information, or assets.  Once all of the assets have their classification labels assigned, you can then assign employees their  security clearance levels that determine which assets they can access.  For example, an employee with a security clearance of top secret can access information with a top  secret label assigned to it.  #  Policies Affecting Management(Cont..)  Companies may use their own internal classification system.  The following are other examples of classification labels:  ■ High/medium/low: Your company may use an internal classification system of low, medium, and high  to rate the security risk if the information is exposed to the public.  ■ Private/public: A simple approach to classifying information is to label the information as either  private or public. Private means that the information is for internal use, while public is information that  does not present a security risk if exposed to the public.  ■ Sensitive: Sensitive data is data that should be protected so that external parties do not have access  to the information. Sensitive data is considered private data.  ■ Confidential: Data should be considered confidential if it could cause significant risk to a business if  accessed by unauthorized persons. Confidential data and sensitive data are terms that are often  interchanged.  ■ Critical: Critical data is the data that is important to business operations. For example, critical data to a  business may be its customer list or product list.  ■ Proprietary :Proprietary information is information that is company owned and should not be shared  outside the company  #  Data Retention Policy:  Data retention policy specifying how long certain information must be retained within the organization. Organizations  may have a retention policy that specifies a number of actions that are performed on data:  ■ Age of data:  Some companies have policies in place specifying that each piece of information must include metadata identifying the creation  date and the expiration date.  This helps someone looking at the data know whether it needs to be retained or can be destroyed, because it is possible that old  data is outdated and inaccurate.  The age limit on data could be three years to seven years, and the retention policy may specify that the data is to be destroyed  after that time.  ■ Retaining data:  Companies should also have policies in place that specify how long information must be retained before it is allowed to be  destroyed.  Many companies have retention periods of up to seven years.  The retention policy should also identify the retention periods for different types of information. For example, accounting data  could have a retention period of seven years, while marketing data could have a retention period of only three years.  The retention policy should also identify where information is archived for long-term storage.  Some data may have a retention category assigned, such as transient data, which is data that does not have to be retained. This  may include items such as voicemails and some types of e-mail.  It should be noted that regulations governing an organization may dictate the retention polices that are required for different types  of information.  #  Other Popular Policies(Cont..)  As mentioned earlier, numerous different policies go into a security policy.  The following are some other popular policies that exist within large organizations:  ■ Remote access policy:  The remote access policy is designed to determine how remote users will gain access to  the network, if at all.  In the remote access policy, you specify remote access protocols that are required to be  used and specific software solutions the company has tested and approved.  You may also specify that the client system must be up to date with patches and antivirus  updates.  ■ Wireless policy:  The wireless policy specifies whether wireless networking is allowed to be used within the  company.  If wireless networking is allowed, the wireless policy specifies the security controls that  should be put in place to secure wireless; for example, whether MAC filtering is used and if  wireless encryption, such as WPA2 or WPA3, is required.  #  Other Popular Policies(Cont..)  ■ VPN policy:  The virtual private network (VPN) policy specifies how remote users will connect to the network using the Internet.  In the VPN policy, you specify which VPN protocol and solution are to be used for remote access via a VPN.  You may also specify that the client system must be up to date with patches and antivirus updates.  ■ Incident response policy:  The incident response policy is designed for the security team that will be handling security incidents.  The incident response policy specifies what each person on the incident response team is responsible for and how  to handle security incidents.  ■ Firewall policy :  The firewall policy specifies the company’s firewall solution and the types of traffic allowed and not allowed to pass  through the firewall.  ■ Virus protection policy:  The virus protection policy specifies which devices and systems require antivirus software to be installed.  It also specifies what settings should be configured within the AV software, such as whether the automatic updating  of virus definitions is enabled and the scheduling of virus scans.  #  Other Popular Policies(Cont…)  ■ Audit policy:  The audit policy is an important policy that specifies where auditing needs to be implemented in the company.  The audit policy should specify what types of servers on the network need auditing enabled and what type of activity  should be audited.  The audit policy should also specify who is to review the logs and how frequently.  ■ Physical security policy:  The physical security policy is designed to specify any physical security controls, such as locked doors, fencing, and  guards, that should be implemented.  It is important to ensure that you control access to servers by placing them in a locked server room.  ■ Software policy:  The software policy specifies which software is approved for the business and indicates what software can and  cannot be installed on the system.  You also want to ensure you indicate in the software policy that software piracy by employees is prohibited.  ■ Backup policy:  The backup policy specifies what type of data needs to be backed up and how frequently.  Administrators will look to the backup policy to determine how they will back up data within the business.  #  Employee Education and  Awareness  #  Password Behavior  When it comes to good password best practices, educate your users on the importance of  having strong passwords and the fact that a simple password can be cracked in seconds.  Explain that a strong password is a password that has at least eight characters, has a mix  of upper- and lowercase characters, and contains numbers and/or symbols. Ensure that  users are not using easy-to-guess passwords or writing their passwords down.  This point should be clearly specified in the password policy.  Also, ensure that users are not sharing their passwords with others and that they are  changing their passwords on a regular basis to help prevent a hacked account from being  used for a long period of time.  Finally, users should not be using the same password they use for other user accounts  because if someone hacks the password for one of the accounts, the hacker can get into all  the accounts.  This applies to accounts used to log on to web sites.  For example, a user shouldn’t have the same password for their bank account,  Outlook.com, Gmail, and Facebook account, as a cracked password means the hacker can  get into all of these accounts  #  Data Handling  Users should also be educated on secure ways to handle data.  Data that is kept on a removable drive should be stored in an encrypted format so that if the  removable media falls into the wrong hands, the data is protected.  Policies should be in place as to what types of removable media are allowed in the business and what  types of information are allowed to be stored on that media.  You must ensure that users review the policy and understand the terms of use for such media.  Be sure to educate your users on the proper destruction of data.  Educate the users that simply deleting the files off the drive does not remove the data from the disk  and that employees must follow the secure disposal of equipment policy to get rid of any devices.  Educate your users on proper destruction of hard copies of data (paper-based printouts) and ensure  there is a shredder available to all users to shred sensitive hard-copy documents when they are no  longer needed.  Educate the users on the fact that hackers will dumpster dive, meaning they will go through the  garbage trying to find sensitive information, which is why documents need to be shredded.  #  Clean Desk Policy  Many organizations implement a clean desk space policy that  requires users to ensure that any sensitive documents are stored  away in a secure location at all times and not left in plain view on  someone’s desk.  It is important to stress to employees what the ramifications of not  following the clean desk policy are and to be sure to perform periodic  checks in the evening by walking around the office to see if anyone  has left sensitive documents in plain view.  Another aspect to a clean desk space policy in highly secure  environments is ensuring that documents are in locked cabinets and  devices such as mobile phones are in locked drawers or filing  cabinets when not being used.  #  Tailgating and Piggybacking  Tailgating and piggybacking are methods intruders use to bypass the physical security  controls put in place by a company.  Tailgating is when an intruder waits until an authorized person uses their swipe card or pass  code to open a door, and then the intruder walks closely behind the person through the  open door without the authorized person’s knowledge.  Piggybacking is when the intruder slips through the door with the authorized person’s  knowledge.  To help prevent tailgating, your organization can use a revolving door or a mantrap.  A mantrap is an area between two interlocking doors in which a person must wait until the first door  completely closes before the second door will open to allow access to the building.  A security guard can monitor the mantrap to make sure only one person enters at a time.  Educate your employees on what to do if someone tries to tailgate, or piggyback, through  an open door.  Most companies tell employees not to open the door if someone is hanging around the  entrance and to ensure the door closes completely after they enter or leave the building.  #  Personally Owned Devices  You should ensure that your security policy and AUP(The  acceptable use policy) cover the company’s policy surrounding  the usage of personally owned devices for business use or  within the company’s network and facility.  This is known as the bring your own device (BYOD) policy.  The security best practice is to not allow usage of personally  owned devices because the company has no right to search or  monitor activity if the device is not owned by the company.  For this reason, it is safest to simply state that no personal  devices are allowed for work-related purposes.  #  Use of Social Networks and P2P Programs  One of the leading security concerns regarding employees’ everyday computer use is their Internet habits at home, in the office, or on a  company laptop.  Two areas of concern are social networking sites and peer-to-peer (P2P) programs that allow users to download music, movies, and  software.  Both social media and P2P downloads can be a way that viruses are spread to the user systems.  The company may perform social media analysis to see if employees are exposing sensitive information about work on social media.  This could be something as simple as taking a picture of them at their desk, and the desk has confidential files open that someone can  view if they zoom in on the picture.  A company may also monitor social media for negative postings about the company.  Be sure to educate your employees on acceptable use of social media such as Twitter, Instagram, and Facebook.  Ensure that employees know not to post company-related information on such sites, and prohibit them from posting pictures of  company parties and other events.  You should also specify in the acceptable use policy the company’s rules regarding the use of social networking sites during work  hours.  Some businesses allow the use of such sites on break or lunchtime, but many people spend more time than they should on such sites,  even during work hours.  Many organizations block these sites at the firewall.  Be sure to keep antivirus software up to date because a large number of viruses are being written in applications used in social  networking sites.  #  Use of Social Networks and P2P  Programs(Cont..)  Peer-to-peer software such as BitTorrent is used to share music, videos,  and software applications on the Internet for the rest of the world to  download.  There are two areas to educate your employees on P2P software use.  First, this is a popular way for hackers to distribute viruses across the  network, which is one of the reasons why P2P software should not be  allowed in the company.  Also, employees should be reminded that they should have antivirus  software up to date on all systems at home.  The second point that should be made in the AUP (The acceptable use  policy) is that downloading or sharing of any copyrighted material (such as  music, movies, TV shows, or software) from the company’s systems and  assets is prohibited. Make it clear that the company has no tolerance for  copyright violations and software piracy.  #  IMPORTANCE OF POLICIES  TO ORGANIZATIONAL  SECURITY  #  Third-Party Risk Management  When a business interacts with other third-party companies or individuals, there is risk to the  company that should be identified.  The following list outlines some key third-party organizations your company may interact with:  Vendors: Vendors are companies you interact with that may supply computer hardware, networking  cable, or even pop for your pop machine in the company cafeteria. It is important to identify the  information that is shared with vendors and ensure the vendor takes steps to guard any sensitive  information.  Supply chain: The supply chain is composed of the different companies that provide materials to  your company for it to deliver its products or services to its customers. Attackers may attempt to  hack into your supply chain to infiltrate your business when the materials are sent into your  company.  Business partners: Your company may have business partners it works with. There is a risk that  the business partners’ systems are compromised so that when they connect to your company  network, the attacker is able to gain access. Steps should be taken to ensure that business partners  only have access to information needed.  #  Common Security Terms need to know  The following are types of agreements you need to be familiar with for the Security+ certification  exam:  Service level agreement (SLA)  An SLA is a contract, or agreement, between your organization and anyone providing services to  the organization.  The SLA sets the maximum amount of downtime that is allowed for assets such as Internet service  and e-mail service and is an important element of the security policy.  It is important to ensure you have an SLA in place with all providers, including Internet providers,  communication link providers, and even the network service team.  Should the provider not meet the SLA requirements, that could warrant looking elsewhere for the  service.  It should also be noted that SLAs are used within a company between the IT department and the  other departments so that the various departments have reasonable expectations regarding quality  of service.  #  Memorandum of understanding (MOU): An MOU is a document that establishes an agreement  between the two parties and specifies their relationship to one another.  Statement of work (SOW): An SOW outlines the type of work a company is being hired for, the  timeline for that work, the cost of the work performed, the payment schedule, and any conditions  related to the work.  Measurement systems analysis (MSA): MSA is a master service agreement, which is a document  used if a company is being contracted to perform work on a regular basis. Instead of creating a  detailed SOW each time, you can put the work details within the MSA, and then the SOW created  for each job would refer to the master service agreement (MSA).  Business partnership agreement (BPA) A BPA is a contract between two or more companies that  identifies the terms of their relationship. The BPA identifies key areas such as capital contributions,  distribution of losses or profit, and duties of each partner.  #  End of life (EOL): A product has reached its end of life when the vendor stops creating that  product. It is typically superseded by a newer version of the product.  End of service life (EOSL) The EOSL marking is typically assigned to hardware or software that is  no longer supported by the vendor. A product that has reached EOSL will no longer have security  updates developed for it by the vendor, which would make that product a risk to your organization.  Nondisclosure agreement (NDA) An NDA is a document that outlines the confidentiality of the  relationship between two parties and what information is considered to be confidential. The NDA  also identifies how confidential information is to be handled during the relationship and after the  relationship has ended.  #  Policies Affecting Data  A number of security policies affect employees’ access to data and how the company manages its  data. The following are some common policies affecting data:  Classification: Data is assigned a security label, and in order for someone to access that  information, they must have that security clearance level. Be sure to review the data classifications  presented earlier in  the chapter when you prepare for the Security+ exam.  Governance: To help minimize security incidents with data, a company should have data  governance policies that determine who has control over the data, as well as how data is handled  within the organization.  Retention: Companies should have retention policies that determine how long data should be  retained. Different types of data may have different retention requirements—for example, financial  records are typically retained for seven years.  #  Credential Policies  Personnel: Each employee within the company should have their own credentials for accessing the  network and computer systems. Employees should be taught security best practices with  credentials, such as not sharing credentials with other employees.  Third party Third-party entities such as business partners or contractors should also have  credentials to access systems that are needed. It is important to follow best practices with these  credentials, such as ensuring that account expiration options are set on contractors’ credentials.  Devices: You may need to manage credentials for devices in a few different ways.  First, you would set passwords on devices so that only authorized persons can access those  devices.  You should also set the idle timeout on each device so that the device automatically locks after  a short idle time.  #  Service accounts: Software that runs on a system also needs  to run as “someone,” so you should create what is known as a  service account for the software. After creating the account, you  then configure the software to use that account to authenticate  to the system. This becomes the security identity of the software  as it accesses resources on the network.  Administrator/root accounts: You should also manage the  credentials of administrator accounts on systems (also known  as root accounts). It is important to ensure that the administrator  account on each system is using a different password so that if  the password is compromised on one system, the same  password cannot be used on the other systems  #  #  Privacy and Sensitive Data Concepts  Organizational Consequences of Privacy and Data  Breaches  A company may face a number of consequences if it finds it has a privacy and data breach. The  following are key consequences to remember for the Security+ exam:  Reputation damage: One of the biggest consequences to a company is reputation damage. If  customers learn that your business is not safeguarding sensitive data, they may decide to no longer  do business with your company. This impacts the financial status of the company and could cause  the company to close.  Identity theft: If unauthorized access to sensitive data occurs, you or your customers may  experience identity theft.  Fines: You could be susceptible to fines for not safeguarding sensitive data properly. These fines  could put financial stress on your company.  IP theft If you have a data breach that results in unauthorized access to sensitive company data, it  could result in the attacker stealing intellectual property.  #  Notifications of Breaches  If a data breach occurs within your business, you will need to notify the appropriate persons. Who  you notify will depend on the type of business you have and the type of security incident that  occurred.  The two different forms of notifications are as follows:  Escalation: After discovering that a security incident has occurred, you may need to report the  incident to the incident response team. After investigating the incident, the incident response team  may need to escalate to another party, depending on the incident. For example, if it is a cloud  incident, they may need to escalate to the cloud service provider.  Public notifications and disclosures: Depending on the regulations and laws governing your  organization, you may need to make a public statement about any security incidents and disclose  the details of the type of information that has been breached. The law may require that the company  individually notify affected users and customers.  #  Data Types  When creating security policies, your goal is to protect privacy and sensitive data within the  organization.  Understanding the types of data that exist within the organization will help you understand the type  of security controls needed. For example, knowing the different classifications of information  discussed earlier in the chapter, such as private and public data, is important to securing that data.  Other types of data found within businesses that need safeguarding are listed here:  Personally identifiable information (PII): PII is any information that can uniquely identify a person.  For example, a driver’s license number is considered PII data. You will learn more about PII  information in the next section.  Health information Health information typically contains confidential medical information about a  person that should only be accessed by authorized individuals, such as a patient’s doctor.  #  Financial information: Financial information such as credit  card numbers and bank account information should be kept  confidential, with steps taken to ensure the data is not stored in  plain text within information systems.  Government data: Information that could present a security  risk to the government if breached should be heavily protected  so that only authorized individuals have access to the  information.  Customer data: Sensitive customer data should be protected  at all times, such as contact details, address information, and  any financial data related to the customer.  #  Privacy Enhancing Technologies  You can use a number of different technologies to help protect different types of sensitive  information, such as credit card numbers and health information.  Data minimization: The first step to securing sensitive data is to minimize the amount of  information you collect. Data minimization is the term used to describe the process of only collecting  information that is necessary.  Data masking: Data masking is a technique used to protect confidential or private data, which  involves replacing characters in the data with nonrelevant characters. An example where data  masking may be used is if you have a consultant working on a database, you supply them a  masked version of the database so that sensitive information found in the data is not available to the  consultant.  Tokenization: The tokenization of data is when sensitive information found in data is substituted  with a nonrelevant data string known as a token. This string is then stored in a data map elsewhere  that can be looked up to convert the token data back to the sensitive data when needed. This is a  common technique used to secure credit card information so that the credit card data is not stored  with the customer data.  #  Anonymization: Anonymization is a data privacy technique that involves  removing personally identifying information from data so that the people  being described in the data can remain anonymous.  Pseudo-anonymization: Also known as pseudonymization,  pseudo-anonymization is when personally identifiable information located  within fields of a database are replaced by a pseudonym.  #  Other Considerations  Information lifecycle: Information has a lifecycle within the business from the time the information  is created, distributed to the employees, used by the employees, maintained, and finally disposed  of.  Impact assessment: An impact assessment is used to evaluate the impact of a security  compromise on the business. For example, what is the impact of the company’s e-commerce site  being hacked and the hacker accessing customer records?  Terms of agreement: Terms of agreement is a document that outlines the rules and conditions of a  relationship between two parties that both parties agree to.  Privacy notice: A privacy notice, also known as a privacy policy, is a statement that communicates  to individuals how the company collects, uses, discloses, manages, and disposes of customer |