UNIT-5 Security Policies

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Contribute to effective cyber security policies in an organizational setting ✓ Identify those responsible for managing and enforcing security policies ✓ Understand every key element of the effective security policy

Unit 5

Security Policies

A free and open Internet is at the heart of the new Cyber Security Strategy by the European Union and the European Commission. The new Communication is the first comprehensive policy document that the European Union has produced in this area. It comprises internal market, justice and home affairs and the foreign policy aspects of cyberspace issues. ENISA has listed all the documents of National Cyber Security Strategies in the EU but also in the world.

For the hardware devices, security policies are rules that are electronically programmed and stored within security equipment to control such areas as access privileges. Security policies are also written or verbal regulations by which an organization operates. In addition, companies must decide who is responsible for enforcing and managing these policies and determine how employees are informed of the rules and watch guards.

What are the policies?

The policies that are implemented should control who has access to which areas of the network and how unauthorized users are going to be prevented from entering restricted areas. Written policies as basic as to warn employees against posting their passwords in work areas can often pre-empt security breaches. Customers or suppliers with access to certain parts of the network, must be adequately regulated by the policies as well.

Who will enforce and manage the policies?

An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access

and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role.

Training

Policies and training can limit the risk

Cybersecurity is a term that has come to encompass a range of concepts including the practice protecting an organization's information, networks, computer, and resources against attacks from security attacks. The term is also used by institutions and government agencies to refer to the act of protecting assets, infrastructure and people against computer attacks.

Cyber security training has become an essential part in developing a team that is capable of and ready to protect and defend an organization, institution, agency, or government entity. The purpose of training is to provide assurance that a certified individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security.

Training people to adopt security conscious behaviors and establishing policies for maintaining a secure environment goes a long way toward improving an organization's overall security posture. The next two sections cover the people and policy dimensions of cyber security.

Cyber Security Policy

The corporate security policy expresses the management's commitment to securing critical assets and provides the framework for developing, implementing, and enforcing security controls. The policy document(s) must be available to all personnel who are required to comply with its requirements. Review and update the policy periodically.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

?	Activity / Security Control	Rationale
	Assign responsibility for developing, implementing, and enforcing cyber security policy to a senior manager. Ensure that the senior	The development and implementation of effective security policies, plans, and procedures require the

	departments to enforce the policy.	collaborative input and efforts of stakeholders in many departments of the organization. Assigning a senior manager to organize and drive the efforts, with the authority to make and enforce decisions at each stage, raises the chances of success.
	Define security-related roles and responsibilities.	Employees at virtually every organizational level have responsibility for some part of developing or applying security policies and procedures. Defined roles and responsibilities will clarify decision-making authority and responsibility at each level, along with expected behavior in policy implementation. Creating a multidisciplinary oversight committee ensures that all stakeholders are represented.
	Identify security aspects to be governed by defined policies.	An effective security program requires policies and procedures that address a wide range of management, personnel, operational, and technical issues.
	Document a brief, clear, high-level policy statement for each issue identified.	The high-level policy statements express three things: The organization management's

		commitment to the cyber security program. The high-level direction and requirements for plans and procedures addressing each area. A framework to organize lower-level documents.
	Reference lower-level policy documents.	Lower-level policies, plans, and procedures provide the details needed to put policy into practice.

	Activity / Security Control	**Rationale**
	Define the implementation plan and enforcement mechanisms.	A careful rollout of the program, well-documented policies that are accessible to the personnel they affect, and clearly communicated consequences of violating policies will help ensure compliance.
	Define a policy management plan.	This will help maximize compliance by providing mechanisms to: Request, approve, document, and monitor policy exceptions. Request, approve, implement, and communicate changes to policies, plans, and procedures.

Security Policy Elements

The security policy should address the following, where applicable:

1. Policy management
    - Purpose, scope, and applicability
    - Roles and responsibilities
    - Implementation and enforcement procedures
    - Exceptions
    - Policy reviews, approvals, and change management
2. Personnel and training
    - Personnel risk assessment
    - Security awareness program
    - Cyber security training
3. Critical asset management
    - Methodology for identifying critical cyber assets
    - Inventory and classification of cyber assets
    - Information protection and data privacy
    - Cyber vulnerability assessment
    - Access control, monitoring, and logging
    - Disposal or redeployment of assets
    - Maintenance and change control of the asset inventory and classifications
4. Electronic security perimeter (ESP)
    - Critical assets within the perimeter
    - Cyber vulnerability assessment
    - Access control, monitoring, and logging
    - Configuration, maintenance, and testing
    - Documentation maintenance to support compliance
5. Physical security
    - Critical assets within the perimeter
    - Access control, monitoring, and logging
6. Incident reporting and response
7. Disaster recovery and business continuity plans

Most of these topics are expanded in other sections of this guide. Note that the master security policy document may address some topics briefly and reference lower-level security policy documents, such as the following:

- Human Resources Security Policy and Procedures
- Guidelines for Handling Sensitive Information Assets
- Physical Security Policy and Procedures

- Disaster Recovery and Business Continuity Plans and Procedures
- Asset Disposal Procedures
- Encryption Standard and Usage Guidelines
- Third-Party Software and Service Provider Standard
- Configuration Standards
- Data Backup Standard

Security-Related Roles and Responsibilities

Everyone in the organization has a role in maintaining security. Define and document the roles and responsibilities of at least the following:

- The governing body for the security policy, e.g., an oversight board comprising representatives of stakeholder groups (engineering, legal, IT, etc.).
- A designated information security manager who maintains the policy and provides guidance for implementation and enforcement.
- Department managers who "own" the critical cyber assets and are responsible for implementing the security policies and procedures to protect those assets.
- Personnel with authorized access to critical assets who must review, provide feedback on, and comply with security policies.

Policy Implementation and Enforcement

Implementation and enforcement of security policies and procedures require defined processes to disseminate them effectively, ensure that they are understood and are available at all times, and enforce compliance (e.g., through audits and disciplinary actions for noncompliance).

Over time, organization or environmental changes will require changes to the security policy. Defined and documented processes for requesting, evaluating, and approving changes will ensure that the policy remains current and relevant.

Policy Exceptions

Policy exceptions occur for a variety of reasons. Simple examples include an overriding business need, a delay in vendor deliverables, new regulatory or statutory requirements, and temporary configuration issues. The exception process must ensure these circumstances are addressed in a manner that makes all stakeholders aware of the event, the risks, and the timeline for eliminating the exception.

Personnel and Training

Insufficiently trained personnel are often the weakest security link in the organization's security perimeter and are the target of social engineering attacks. It is therefore crucial to provide adequate

security awareness training to all new hires, as well as refresher training to current employees on a yearly basis.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

☐	**Activity / Security Control**	**Rationale**
	Adequately vet candidates for hire.	Provide a level of confidence that new hires are trustworthy.
	Establish a security-awareness program.	Ensure that all personnel have an understanding of sensitive information, common security risks, and basic steps to prevent security breaches. Further, ensure that personnel develop habits that would make them less susceptible to social engineering attacks.
	Train employees who have access to protected assets.	Ensure that employees who have electronic or physical access to critical assets know how to handle the assets securely and how to report and respond to cyber security incidents.
	Enforce “least privilege” access to cyber assets and periodically review access privileges.	Ensure that employees have only the privileges they need to perform their jobs.

Security Awareness and Training

The organization must establish, document, implement, and maintain a security awareness program for all personnel. The awareness program describes common security risks and how to avoid them. Awareness reinforcement should occur at least quarterly.

For personnel having authorized cyber access or authorized unescorted physical access to critical cyber assets, the organization should establish a training program that includes at least the following:

- The policies, access controls, and procedures developed for critical cyber assets.
- The proper use of critical cyber assets.
- The proper handling of critical cyber asset information.

Action plans and procedures to recover or reestablish critical cyber assets, and the required access to these assets, following a cyber security incident

Due Diligence in Hiring

Diligence in the hiring and personnel review process is crucial. It is important to define and document a risk assessment program for personnel with authorized cyber access or authorized unescorted physical access to critical cyber assets. The program must comply with applicable laws and existing collective bargaining agreements. The risk assessment must include, at a minimum, identity verification and a seven-year criminal check. This information must be updated at least once every seven years (or for cause).

In addition, ensure that third-party vendors enforce similar checks for their personnel.

Access Privileges

Grant each employee the *lowest* levels of access to cyber assets and other privileges needed to do his or her job efficiently.

Maintain a list of all personnel who have authorized cyber access or authorized unescorted physical access to critical cyber assets. This list must include each person's specific electronic and physical access rights to such assets. Review the list quarterly and update it within seven days of any change in a list member's access rights.

Operational Risks

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions following the checklist in the body of the section.

☐	Activity / Security Control	Rationale
	Perform periodic risk assessment and mitigation, including threat analysis and vulnerability assessments.	Maintain a fresh picture of the effectiveness of the organization's security control versus threats facing the organization.
	Control, monitor, and log all access to protected assets.	Prevent unauthorized access to assets; detect unauthorized access to assets; enforce accountability.
	Redeploy or dispose of protected assets securely.	Ensure that the redeployment or disposal of cyber assets does not inadvertently expose sensitive information to unauthorized entities.
	Define and enforce secure change control and configuration management processes.	Ensure that system changes do not "break" security controls established to protect cyber assets.
	Create and document incident-handling policies, plans, and procedures.	Ensure that the organization is prepared to act quickly and correctly to avert or contain damage after a cyber security incident.
	Create and document contingency plans	Ensure that the organization is prepared to act

	and procedures.	quickly and correctly to recover critical assets and continue operations after a major disruption.
	Train employees in incident-handling and contingency plans.	Ensure that personnel responsible for responding to cyber incidents or major disruptions have a firm grasp of the response plans and can execute them under stress.

Contingency Planning

A **contingency** is any unplanned outage or failure of a system component. In addition to an incident-handling plan, organizations need policy, plans, and procedures for disaster recovery, continuity of operations, and possibly other contingency plans. Policy and plans must include preparation and training for responding to an emergency along with detailed procedures for executing defined strategies.

A **disaster recovery plan applies** to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. It includes the preparation (e.g., off-site storage of system backups), emergency facilities, and procedures for restoring critical cyber assets and infrastructure at an alternate site after an emergency.

A **business continuity plan** focuses on sustaining an organization's mission/business functions during and after a disruption. A business continuity plan may be written for mission/business functions within a single business unit or may address the entire organization's processes.

Continuity and recovery plans define interim measures that increase the speed with which organizations resume service after disruptions. These plans must be tailored to each system. Creating specific measures requires a detailed understanding of specific scenarios.

Table 3. Impacts and Mitigations for People and Policy Risks[13]

People and Policy Risks	Potential Impact	Mitigations
Inadequate security training and awareness.	Insufficiently trained personnel may inadvertently provide the visibility, knowledge, and opportunity to execute a successful attack. An inadequately trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited. They may, for example: • Insert malicious USB sticks found in the parking lot into machines with access to control systems, providing attackers control over the control systems. • Hold the door for potential attackers carrying a big box entering a "secured premise," allowing them unauthorized access and physical proximity to critical / control systems. • Surf porn sites, which often compromise workstations with bots or worms.	Ensure that the security training and awareness program is adequate to address the risks resulting from insecure behavior of employees. Ensure that all employees undergo security training when hired and at least once a year thereafter. The degree and nature of security training for personnel may vary based on their job function.

	Fail to respond to someone capturing wireless network traffic on the front lawn or parked in the guest parking lot. Be careless with ID badges and credentials that can be leveraged to gain access to critical machines.	
Insufficient identity validation, background checks	The human factor must always be considered the weakest element within any security posture; identity validation and background checks are measures that are imperative in managing this risk. As the amount and sensitivity of the information one is given responsibility for increases, consideration should be given to requiring separation of duties to ensure that no one individual is given the "keys to the kingdom."	Institute appropriate procedures to conduct background checks of all new hires. Further, prior to being granted access to sensitive information and resources, proper authentication and authorization mechanisms are required. The latter first verifies the identity of the party requesting access and then confirms that this party is authorized to access resources to which access is being requested.

People and Policy Risks	**Potential Impact**	**Mitigations**
Inadequate security policy.	Vulnerabilities are often introduced due to inadequate or lacking policies. Policies need to drive operating requirements and procedures.	Ensure that security policies adequately cover all aspects of maintaining a secure environment.

Inadequate privacy policy.	Insufficient privacy policies can lead to unwanted exposure of employee or customer / client personal information, leading to both business risk and security risk.	Ensure that the privacy policies adequately cover all aspects of safeguarding access to private information.
Inadequate security oversight by management.	A lack of clear senior management ownership of a security program makes it almost impossible to enforce the provisions of the program in the event of a policy being compromised or abused.	Ensure that a senior manager is assigned responsibility for the overall security program at your organization. Empower this individual to make decisions to refine and enforce the security policies.
Improper revocation of access.	Failure to ensure that employee access is revoked when no longer needed may result in unauthorized access.	Ensure that employees have access to resources and systems only as needed to perform their job function and only for the duration that this need exists. Revoke all access for terminated employees before notifying them of termination.
People and Policy Risks	**Potential Impact**	**Mitigations**
Inadequate security policy.	Vulnerabilities are often introduced due to inadequate or lacking policies. Policies need to drive operating requirements and procedures.	Ensure that security policies adequately cover all aspects of maintaining a secure environment.
Inadequate privacy policy.	Insufficient privacy policies can lead to unwanted exposure of employee	Ensure that the privacy policies adequately cover all

	or customer / client personal information, leading to both business risk and security risk.	aspects of safeguarding access to private information.
Inadequate security oversight by management.	A lack of clear senior management ownership of a security program makes it almost impossible to enforce the provisions of the program in the event of a policy being compromised or abused.	Ensure that a senior manager is assigned responsibility for the overall security program at your organization. Empower this individual to make decisions to refine and enforce the security policies.
Improper revocation of access.	Failure to ensure that employee access is revoked when no longer needed may result in unauthorized access.	Ensure that employees have access to resources and systems only as needed to perform their job function and only for the duration that this need exists. Revoke all access for terminated employees before notifying them of termination.

Table 5. Impacts and Mitigations for Operational Risks[17]

Operational Risks	Potential Impact	Mitigation
Inadequate patch management process.	Missing patches on firmware and software have the potential to present serious risk to the affected system.	Automate the mechanism of monitoring and receiving alerts when new security patches become available. Make sure that security patches are applied at least weekly or more often as appropriate.
Unnecessary system access.	System access that is not managed can result in personnel obtaining, changing, or deleting information they are no longer authorized to access. Related problems include: • Administrators with false assumptions of what actions any one user may be capable. • One user (or many individual users) with sufficient access to cause complete failure or large portions of the electric grid. • Inability to prove responsibility for a given action or hold a party accountable. • Accidental disruption of service by untrained individuals. • Raised value for credentials of	Periodically review the access lists for each critical resource or system to ensure that the right set of individuals has authorized access. Establish standards procedures and channels for granting and revoking employee access to resources or systems.

	seemingly insignificant personnel.	
Inadequate change and configuration management.	Improperly configured software/systems/devices added to existing software/systems/devices can lead to insecure configurations and an increased risk of vulnerability.	Ensure that all hardware and software are configured securely. When unclear, seek further clarification from vendors as to secure settings and do not assume that shipped default settings are secure. Establish change management and approval processes for making changes to the configuration to ensure that the security posture is not jeopardized.
Operational Risks	**Potential Impact**	**Mitigation**
Inadequate periodic security audits.	The audit process is the only true measure by which it is possible to continuously evaluate the status of the implemented security program in terms of conformance to policy, to determine whether there is a need to enhance policies and procedures, and to evaluate the robustness of the implemented security technologies. Failure to perform periodic security audits may lead to unidentified security risks or process gaps.	Ensure periodic security audits that focus on assessing security controls at the various levels, such as people and policy, operational, network, platform, application, process, physical security, and third-party relationships.

Inadequate continuity of operations and disaster recovery plan.	An inadequate continuity of operations or disaster recovery plan could result in longer-than-necessary recovery from a possible plant or operational outage.	It is essential to ensure within the various plant/system disaster recovery plans that are in place that an associated cyber contingency plan and cyber security incident response plan is developed. Each plant/system disaster recovery plan should highlight the need to determine if the disaster was created by or related to a cyber security incident. If such is the case, then part of the recovery process must be to ensure cyber incident recovery and contingency activities are implemented. This means taking added steps like validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc.
Inadequate risk assessment process.	Lack or misapplication of adequate risk assessment processes can lead to poor decisions based on inadequate understanding of actual risk.	A documented risk assessment process that includes consideration of business objectives, the impact to the organization if vulnerabilities are exploited, and the determination

		by senior management of risk acceptance is necessary to ensure proper evaluation of risk.
Inadequate risk management process.	Lack of an adequate risk management process may result in the organization focusing its resources on mitigating risks of little impact or likelihood, while leaving more important risks unaddressed.	Ensure that the organization's risk management process uses the results of the risk assessment process to initiate the timely and appropriate mitigation of risks in a fashion commensurate with their likelihood and impact. A systematic approach should be developed; an executive dashboard needs to show all risks where mitigations are past due.
Inadequate incident response process.	Without a sufficient incident response process, time-critical response actions may not be completed in a timely manner, leading to the increased duration of risk exposure.	An incident response process is required to ensure proper notification, response, and recovery in the event of an incident.

Physical Security Risks

Physical security measures aimed at protecting critical infrastructure of the smart grid are of paramount importance and form a key element of the overall security strategy. While other controls need to exist for defense in depth in case the adversary is successful in gaining physical access, physical security concerns should not be underestimated.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

?	**Activity / Security Control**	**Rationale**
	Document, implement, and maintain a physical security plan.	Ensure that physical security is considered in a structured manner that can be tracked.
	The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times.	Ability to detect unauthorized access attempts. Take appropriate action if unauthorized access occurred.
	All physical access attempts (successful or unsuccessful) should be logged to a secure central logging server.	Ability to detect unauthorized access attempts. Take appropriate action if unauthorized access occurred.
	Physical access logs should be retained for at least 90 days.	Ability to perform historical analysis of physical access.
	Each physical security system must be tested at least once every three years to ensure it operates correctly.	Ensure that proper physical security posture is maintained.
	Testing and maintenance records must be maintained at least until the next testing cycle.	Ability to understand what was tested and improve testing procedures.
	Outage records must be retained for at least one calendar year.	Ability to investigate causes of outages and tie them to unauthorized physical access.

Plan and Protection

Senior managers must document, implement, and maintain a physical security plan. This plan must address, at a minimum:

- The protection of all cyber assets within an identified physical security perimeter or by way of alternate measures if a completely enclosed border is not feasible.
- The identification of all physical access points past the physical security perimeter and measures to control entry at those access points.
- Processes, tools, and procedures to monitor physical access to the perimeter(s).
- Appropriate use of physical access controls.
- Review of access authorization requests and revocation of access authorization.
- A visitor control program for personnel without authorized unescorted access to a physical security perimeter.
- Physical protection from unauthorized access and a location within an identified physical security perimeter for cyber assets that authorize or log access or monitor access to a physical or electronic security perimeter.
- Documentation and implementation of operational and procedural control to manage physical access at all access points at all times.

Monitoring, Logging, and Retention

The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times. Unauthorized access attempts must be reviewed immediately and handled in accordance with procedures. Logging will be sufficient to uniquely identify individuals and the time of access. Physical access logs should be retained for at least 90 calendar days.

Maintenance and Testing

Each physical security system must be tested at least once every three years to ensure it operates correctly. Testing and maintenance records must be maintained at least until the next testing cycle. Outage records must be retained for at least one calendar year.

The tables below summarize physical security risks, impacts, and mitigations.

Addressing Technology Risks

Information technology (IT) is at the heart of the smart grid. As its spreading use helps the smart grid achieve higher operational efficiencies, it also makes the electrical grid more vulnerable to cyber

security attacks. It is therefore important to ensure that the way in which IT is used does not inadvertently provide new avenues of attack to an adversary. Further, IT itself should be applied to institute security controls that will help guard the smart grid ecosystem against successful attacks, as well as enhance the system's ability to detect, isolate, and recover from breaches of security.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

	Activity / Security Control	**Rationale**
	Restrict user-assigned devices to specific network segments.	Least privilege through network segmentation.
	Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic moving from network segment to another of a different security level should default to a "deny all" stance.	Provide security by default.
	Requests for allowing additional services through a firewall or other boundary protection mechanism should be approved by the information security manager.	Centrally manage access according to business need.
	The flow of electronic communications should be controlled. Client systems should communicate with internal servers; these internal servers should not communicate directly with external	Confine sensitive electronic communication to established trust zones.

systems, but should use an intermediate system in your organization's DMZ. The flow of traffic should be enforced through boundary protection mechanisms.	
Protect data in transit.	Preserve the confidentiality and integrity of data in transit.
Protect domain name service (DNS) traffic.	Ensure that data is routed to the right parties.
Use secure routing protocols or static routes.	Avoid the disclosure of information on internal routing.
Deny use of source routing.	Prevent denial-of-service attacks.
Use technologies like firewalls and virtual local area networks (VLANs) to properly segment your organization's network in order to increase compartmentalization (e.g., machines with access to business services like e-mail should not be on the same network segment as your SCADA machines). Routinely review and test your firewall rules to confirm expected behavior.	Achieve network segmentation to achieve compartmentalization.
Separate development, test, and production environments.	Avoid production data leaks into test environments. Have controls in place around access to and changes in the production environment.
Ensure channel security of critical communication links with technologies like Transport Layer Security (TLS). Where possible, implement Public Key Infrastructure (PKI) to support two-way mutual certificate-based authentication between nodes on your network.	Secure data in transit.

Ensure that proper certificate and key management practices are in place. Remember that cryptography does not help if the encryption key is easy to compromise. Ensure that keys are changed periodically and that they can be changed right away in the event of compromise.	Ensure that cryptographic protection is not undermined through improper certificate or key management.
Ensure confidentiality of data traversing your networks. If channel-level encryption is not possible, apply data-level encryption to protect the data traversing your network links.	Secure data in transit.
Ensure integrity of data traversing your networks through use of digital fingerprints and signed hashes. If TLS is not used, ensure that other protections from man-in-the-middle attacks exist. Use time stamps to protect against replay attacks.	Preserve data integrity.
Ensure availability of data traversing your networks. If a proper acknowledgement (ACK) is not received from the destination node, ensure that provisions are in place to resend the packet. If that still does not work, reroute the packet via a different network link. Implement proper physical security controls to make your network links harder to compromise.	Detect failures and promote fault tolerance.
Ensure that only standard, approved, and properly reviewed communication protocols are used on your network.	Use proven protocols that have been examined for security weaknesses.

Use intrusion detection systems (IDSs) to detect any anomalous behavior on your network. If anomalous behavior is encountered, have a way to isolate the potentially compromised nodes on your network from the rest of the network.	Detect intrusions.
Ensure that sufficient number of data points exist from devices on your network before the smart grid takes any actions based on that data. Never take actions based on the data coming from network nodes that may have been compromised.	Avoid taking actions based on incorrect data.
Ensure that all settings used on your network hardware have been set to their secure settings and that you fully understand the settings provided by each piece of hardware. Do not assume that default settings are secure.	Secure configuration.
Disable all unneeded network services.	Reduce attack surface.
Routinely review your network logs for anomalous / malicious behavior via automated and manual techniques.	Detect intrusion.
Ensure that sufficient redundancy exists in your network links so that rerouting traffic is possible if some links are compromised.	Ensure continuity of operations.
Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., nonshared) credentials.	Enforce accountability.

Limit remote access to your networks to an absolute minimum. When required, use technologies like Virtual Private Networks (VPNs, IPSec) to create a secure tunnel after properly authenticating the connecting party using their individual credentials. In addition to a user name and password, also use an RSA ID-like device to provide an additional level of authentication.	Prevent unauthorized access.
Implement remote attestation techniques for your field devices (e.g., smart meters) to ensure that their firmware has not been compromised	Prevent unauthorized modification of firmware on field equipment.
Require a heartbeat from your field equipment at an interval known to the piece of equipment and to the server on your internal network. If a heartbeat is missed or comes at the wrong time, consider treating that piece of equipment as compromised / out of order and take appropriate action.	Detect tampering with field equipment.
Ensure that the source of network time is accurate and that accurate time is reflected on all network nodes for all actions taken and events logged.	Maintain accurate network time.
Document the network access level that is needed for each individual or role at your organization and grant only the required level of access to these individuals or roles. All exceptions should be noted.	Maintain control over access to network resources and keep it to a necessary minimum.
All equipment connected to your network should	Control hardware that gets connected to

be uniquely identified and approved for use on your organization's network.
your organization's network.

Network Connection Control

Restrict user-assigned devices to specific network segments

Devices should be authorized for connection to one network segment, but should not be authorized to connect to other network segments (e.g., segments where information of a higher security classification is stored, processed, and/or transmitted and the user of that device has not been granted access to information assets of that classification).

User devices should be specifically prohibited from cross-connecting (i.e., acting as a router) between any two networks.

Firewall

Your organization's firewalls should be configured in accordance with the firewall configuration standard and the policy elements below:

- Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic from one network segment to another of a different security level should default to a "deny all" status.
- Firewalls should be configured to deny any of the following traffic types:
  a. Invalid source or destination address (e.g., broadcast addresses, RFC 1918 address spaces on interfaces connected to public networks, addresses not assigned by IANA on interfaces connected to public networks).
  b. Those destined for the firewall itself, unless the firewall provides a specific service (e.g., application proxy, VPN).
  c. Source routing information.
  d. Directed broadcasts that are not for the subnet of the originator (these can be used to create broadcast storms in denial-of-service attacks against third parties).
  e. Those destined for internal addresses or services that have not been approved for access from external sources.
  f. Requests for allowing additional services through a firewall or other boundary protection mechanisms should be approved by the information security manager.

Flow of electronic communications

The flow of electronic communications should be controlled. Client systems should communicate with internal servers; these internal servers should not communicate directly with external

systems, but should use an intermediate system in your organization's DMZ. The flow of traffic should be enforced through boundary protection mechanisms.

Protecting data in transit

When any nonpublic classified data transits a network and the confidentiality and integrity of that data cannot be guaranteed because of the use of protocols which do not provide a mechanism for protecting the data payload, encryption should be used to guard against disclosure and modification of the data.

Protecting DNS traffic

The domain name service (DNS) should be deployed in a multitier architecture that protects internal systems from direct manipulation. Internal client resolvers should direct their queries to internal DNS servers, which forward all queries for external resource records to DNS server(s) in a DMZ. The flow of traffic should be enforced through boundary protection mechanisms.

Further Reading:

- ✓ ***Cyber Security Policy Guidebook by Jennifer Bayuk, Jason Healey 2012***