

**Blue Team Level 1 Certification
(Standard)** Management Principles 4 Topics | 1 Quiz Section Introduction, Management Principles Risk Policies and Procedures Compliance & Frameworks Activity) End of Section Review, Management Principles**PHISHING ANALYSIS DOMAIN** PA1) Introduction to Emails and Phishing 7 Topics | 1 Quiz PA2) Types of Phishing Emails 10 Topics | 2 Quizzes PA3) Tactics and Techniques Used 12 Topics | 2 Quizzes PA4) Investigating a Phishing Email 8 Topics | 2 Quizzes PA5) Analysing URLs, Attachments, and Artifacts 8 Topics | 1 Quiz PA6) Taking Defensive Actions 12 Topics | 1 Quiz PA7) Report Writing 7 Topics | 1 Quiz PA8) Phishing Response Challenge 3 Topics | 1 Quiz**THREAT INTELLIGENCE DOMAIN** TI1) Introduction to Threat Intelligence 7 Topics TI2) Threat Actors & APTs 6 Topics | 2 Quizzes TI3) Operational Threat Intelligence 7 Topics | 1 Quiz TI4) Tactical Threat Intelligence 7 Topics | 2 Quizzes TI5) Strategic Threat Intelligence 5 Topics | 1 Quiz TI6) Malware and Global Campaigns 6 Topics | 1 Quiz**DIGITAL FORENSICS DOMAIN** DF1) Introduction to Digital Forensics 5 Topics DF2) Forensics Fundamentals 10 Topics | 5 Quizzes DF3) Digital Evidence Collection 8 Topics | 1 Quiz DF4) Windows Investigations

Policies and Procedures

Blue Team Level 1 Certification (Standard) > Management Principles > Policies and Procedures

COMPLETE

This lesson will cover what policies and procedures are, why they're used, and provide some examples so you can become familiar with these administrative security controls and management concepts. Policies and procedures are an extremely important part of cybersecurity, and are used every single day, helping to reduce threat by stating what employees can and can't do, and provide documentation on how activities should be conducted.

POLICIES

A policy is a plan of intent or course of action towards a particular domain. This could be a country's attitude towards an issue or a business's plan of responsibility. Policies guide actions in many ways. Some policies are laws or regulations whereas some are principles, direction, or guidelines. They range in complexity, from home to office and government. Policies are at the highest level, followed by procedures and standards, and then guidelines.

WHY ARE THEY USED?

A policy outlines rules and provides principles that guide the actions to be taken, it will set out roles and responsibilities that can be accountable.

You have followed policies all your life and may never have thought of it. For example, "No TV until homework is done" or "bedtime at 8 pm", these are policies commonly laid down by parents. These are simple and easy to understand; consequences may include loss of TV privileges or no treats. Policies laid down in business and government will be more complex and have more serious consequences. For example, an insurance policy is a very detailed agreement between you and the insurance provider.

Polices may also be a collection of policies, an IT Security policy will have other policies pertaining to it. Any new employee will be expected to, read, and sign an acceptable use policy to use company assets. It may also include a policy on the use of personal devices. Knowing and understanding an organization's policy is vital to operations, most companies will have many policies. A good practice is to have a detailed knowledge of the policies relevant to your roles and responsibilities, but to be aware of other policies and know where to seek guidance on them as they are often interlinked.

COMMON POLICY EXAMPLES

Acceptable Use Policy (AUP)

This is a document that stipulates what a user can and cannot do on a corporate, university or internet service provider (ISP) network and /or internet access. The user agrees to the terms laid out by the policy to gain access to the network. A code of conduct governs the behavior of the user while using the network/internet provided to them; such as no social media or adult content. These policies should outline the consequences in case a user

3 Topics 3 Quizzes

violates this agreement, for example, loss of internet privileges or suspension of the account.

Service Level Agreement (SLA)

A service level agreement lays out a set level of commitment between a service provider and a customer. For example, an internet service provider or cloud provider will have included a service level agreement when you take out their services. This will dictate; services provided, performance levels, resolution response times, repercussions if the service is not provided.

Bring Your Own Device (BYOD)

This is a policy that outlines the usage of a personally owned device on a corporate network, such as a laptop or mobile phone.

Memorandum of Understanding (MOU)

A Memorandum of Understanding is a document that formally outlines an agreement between two or more parties but, is not legally binding. An MOU is usually a sign that a binding contract is imminent.

STANDARD OPERATING PROCEDURES

A standard operating procedure is a step-by-step set of instructions developed for a routine task. They provide specific technical processes and techniques used to complete a set task. This ensures tasks are performed effectively and efficiently while reducing errors, miscommunication, and failure to comply with regulations. If all members of a team or organization use the same SOP this creates uniformity within the organization. An SOP can be written for almost any task and are periodically reviewed and developed. Any SOP should be tested prior to being put into practice. Once in practice, they should be easily accessible throughout the organization.

Standard operating procedures may have local or branch variations. This could be to comply with regulations in different areas such as state laws in the US; or when including specific establishments that are local to your branch or office, potentially a local distributor. These variations do not distract from the set of instructions being used; they are the standard in your environment. You may often find a head office will set the policy, but your local management will design the SOP. Good SOPs are designed with input from those using them to give a complete picture of the tasks they are outlining.

[Previous Topic](#)

[Back to Lesson](#)

[Next Topic](#)

[Privacy & Cookies Policy](#)

