



Prepared by:

*Nouman Ali*

[MANUAL OVERVIEW 4](#_Toc59138386)

[SECTION 1: Introduction: Welcome to CyberLeet 6](#_Toc59138387)

[1.1 Introduction 7](#_Toc59138388)

[1.2 Your Role at CyberLeet 9](#_Toc59138389)

[1.3 Purpose of This Manual 10](#_Toc59138390)

[SECTION 2: Core Tenets of Cybersecurity 11](#_Toc59138391)

[2.1 Confidentiality 11](#_Toc59138392)

[2.2 Integrity 12](#_Toc59138393)

[2.3 Availability 13](#_Toc59138394)

[SECTION 3: Cybersecurity Policies 15](#_Toc59138395)

[3.1 Password Policies 16](#_Toc59138396)

[**3.1 Password Policies** 16](#_Toc59138397)

[3.2 Acceptable Use Policies 18](#_Toc59138398)

[3.3 User Training Policies 19](#_Toc59138399)

[3.4 Basic User Policies 20](#_Toc59138400)

[SECTION 4: Threat Mitigation Scenarios 23](#_Toc59138401)

[In addition to every member on board, company property will only be available to employees unless permitted by the right authorities within the company. Upper management will log and track any visitation to ensure that every event is accounted for. Employees who require remote access via VPN or RAP to continue to work outside the company are determined by upper-management and reasoning would play a big factor in granting that privilege. Remote access should only be approved to meet deadlines and complete special projects. The ability to obtain remote access will be limited and not offer to every member of the organization. 25](#_Toc59138402)

[4.2 Malware 26](#_Toc59138403)

[4.3 Your Choice 27](#_Toc59138404)

[SECTION 5: References 28](#_Toc59138405)

# MANUAL OVERVIEW

You are the training manager at CyberLeet Technologies, a midsized firm that provides cybersecurity services to other businesses. CyberLeet’s core customer base is sole proprietorships and other mom-and-pop shops that are too small to have their own IT departments and budgets. Generally speaking, your clients have a reasonably high risk tolerance, and put a premium on the functionality of their IT systems over stringent security measures. However, you also have clients that must protect highly sensitive information in order to continue operating successfully. For example, CyberLeet supports a few small public-accounting firms that need to maintain important tax-related information, as well as several day-care businesses that must keep children’s health records private while allowing necessary access for certain caregivers. In the past year, CyberLeet has experienced rapid growth, which means you can no longer personally provide one-on-one training to every new information security analyst as they are hired. Therefore, you have decided to create a training manual that will explain to the current and future cohorts of new hires the essential principles and practices that they must understand in order to be successful in their role as information security analysts at CyberLeet.

Manual Layout

There are four sections in the manual, which cover all the components of a new employee training manual. As the training manager, you must complete each section using information you learned in this course. Refer to the background information on CyberLeet and apply the appropriate information that best matches based on the size of the company, the value of cybersecurity, and its core tenets. Apply best practices of cybersecurity principles for addressing the common threat scenarios of a sole proprietary business. The main sections of the manual you are responsible for completing are the following:

* Introduction
* Core tenets of cybersecurity
* Developing cybersecurity policies
* Threat mitigation scenarios

In Section One, describe the organization. Provide a short history of the company, define the way it operates, and describe its place within the industry and the community it serves. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

# SECTION 1: Introduction: Welcome to CyberLeet

|  |
| --- |
| 1.1 Introduction Here at Cybernet Technologies, we take pride in ourselves on being a security firm that gives our clients the utmost will to secure their business with the sense of comfort instilling trust within our company. As a representative of Cybernet Technologies, our main goal is to provide quality services and to ensure that top-notch security is taken to secure our client's business on all levels. We will safely keep our client's information and guarantee that all measures are taken to secure all data given, taken, and stored within the company. It is our job to upkeep the advancement of technology and considers all possibilities when it comes to threats in cybersecurity ensuring our team is up to date and aware of the world's threats today.  Today there is a high demand for the need of cybersecurity experts/specialists due to the rise of cybersecurity threats/breaches. There has been an incline of cyber-attacks that happen daily throughout the world. It’s essential that people are aware of these threats and made aware of why it is important to gain some knowledge to help protect their equipment. Personal equipment would range from personal computers/laptops, cell phones, and other smart devices. |

|  |
| --- |
| 1.2 Your Role at CyberLeet The information security analyst role is a critical position to which the candidate will be in charge of the responsibility to the task assigned to them. Listed below you will find the job duties/requirments of the job at hand.   * Planning and implementing a POA (Plan of Action) to secure and protect any or all computer systems, networks, and sensitive data in any case scenario. * Staying up-to-date with the latest intelligence, newer threats to include hackers’ methodologies, tactics, and events. * Carrying out risk assessments along with testing of data processing systems in the detection of phishing threats. * Monitor the user's rights to ensure correct access is granted to each employee. * Installing firewalls, data encryption, and other security measures to our infrastructure, network, etc. * Forensics analysis and research to stay updated with cause, solve, and resolution. * Creating, testing and implementing network disaster recovery plans along with tracking statuses to generate * Staying up-to-date on the latest intelligence, including hackers’ methodologies * Preventing data loss and service interruptions by researching new technologies that will effectively be protecting the companies network * Communicate with our clients in the event of any security breach/attacks and shutdown processes or update clients about system updates. |

|  |
| --- |
| 1.3 Purpose of This Manual This manual was created to help our new employees understand how critical and essential it is to hold the title: all information security analysts. The company requires security analysts to abide and follow all these guidelines on cybersecurity. The hire would be able to address vulnerabilities, threats, and how to resolve these issues. These policies are in place to address and protect sensitive and non-sensitive data from any unauthorized access, corruption, or disclosure. The hire must understand their roles and play a key element in the security of the companies overall platform. Overall he or she must be able to provide quality professional work ethics and maintain their daily job duties along with the ability to respond to any worst-case scenario. |

A widely applicable security model is the CIA triad, standing for confidentiality, integrity, and availability. There are three key principles that should be guaranteed in any kind of secure system. In Section Two, describe the significance of each area as directed in each designated area. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

# SECTION 2: Core Tenets of Cybersecurity

|  |
| --- |
| 2.1 Confidentiality There are three parts of the triad, confidentiality, integrity, and availability (CIA). The first part of the triad (confidentiality) confidentiality means something that is secret and is not supposed to be disclosed to unintended people or entities. Procedures should be in place to safeguard sensitive material from reaching the wrong individuals, which is critical while ensuring that the right person has access to the confidential information. Information should and always remain restricted to those who are not authorized to receive it.  For example, if the information is to be categorized by the volume of sensitive material and restricted by clearance. The information obtained by the wrong people or person could be used for blackmail, Ransom, or even far worst scenarios than that. Procedures can then be executed according to those categories. Data encryption is critical which a shared method to protect confidentiality is. A good standardization would be the implementation of User IDs and passwords that have multiple steps. An eight-character minimum length which would could one lower case letter, one upper case letter, a number, and a special character combined with a two-factor authentication layer. In addition to this process, key fobs and soft tokens could be added as well. There could also be company identification cards upon sign-on, even a biometric reader would further and harden the security aswell. Users must maintain and be responsible for their passwords. If their identity was to be stolen then data and the confidentially of the system would be vulnerable to those who have access to it. |

|  |
| --- |
| 2.2 Integrity The second tenet of cybersecurity, which is “Integrity” the "I" in the "CIA". Integrity is defined as: involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. It is important that any information being stored, added, or even deleted does not go through any alterations unless authorized by the correct personnel. Permission should always be granted prior beforehand, for example, if a user is altering any configuration to a system such as a server, software, hardware or even a file. Any type of modification to a server could give access to an unauthorized entity internal or external within the company. Any software modification could change any security settings in place and alter the levels of security that software may provide. Hardware modifications could also open up doors physically to those who can install unwanted software, or even steal sensitive material. It is essential to keep everything configured correctly without any adjustments unless authorized so that users or outside access could be prevented. |

|  |
| --- |
| 2.3 Availability Availability is the las "A" in "CIA" and is the third tenet in the triad. Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and the correct format. It safeguards the hardware that is maintained and kept up to date to ensure that any downtime is at a minimum. It also works hand in hand with all software required for the device that is working correctly with the operating system as its platform to avoid issues. All software must be kept updated and maintained frequently. Available hardware as a backup is critical as well to reduce downtime to a minimum. A disaster recovery plan should be in place in case of an emergency which will have a definite response time to resolve issues as it comes. In addition to a backup plan, a backup site should be located elsewhere secured in an all-weather location as a secondary plan. Overall availability should be locked down and hardened to prevent any physical intrusion aswell. USB ports, recordable drives may also be used as a way to breach this tenet and should not be overlooked. |

Creating effective cybersecurity policies will make visible changes to how the organization operates. Rely on the information presented in this course to develop the necessary standards and frameworks of effective cybersecurity policies. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

# SECTION 3: Cybersecurity Policies

|  |
| --- |
| 3.1 Password Policies**3.1 Password Policies** The organization's computer systems protection is critical. Protection must be provided from any unauthorized access, from all users, and any physical intrusion. Every user should maintain a password to gain access to the system. The password criteria should be difficult with guidelines that should be followed and met. Every password created must contain a minimum of numbers, special characters, and at least one upper case letter. The password will be in place in conjunction with a unique/creative user ID sign-on should never be duplicated and kept safe as the user's responsibility. The ID will be utilized to authenticate the user’s identification to gain access to the network. All users must upkeep with their password and the password must remain confidential on all levels. Each user must practice safe keeping and should not expose any hints, letters, or naming schemes to reveal any clues regarding their password. Any duplication of any kind would be flagged by the system and would not be accepted at the end of the system. listed below is a criterion that should be met by all users.   * All first initial passwords will be allocated by the company’s system administrator, and must be changed within two hours of activation upon the first attempt to logon. * Passwords must have a 10 length requirement, which should include one number, one special character, one lower case letter, one uppercase letter. * Numerical values should unique and not in sequence. For example 14289 vs. 123456. * All Passwords will be active for 60 days and must be changed 48 hours before expiration. * The system will identify any re-use passwords and will not allow the user to re-use similar patterns when updating their password. * The systems of Password history will be definite until the user is in-active. * After five (3) unsuccessful login attempts, the system will lock out the user and will require assistance from the systems administrator.            It is critical to enforce this strong password policy, the integrity of the organization is essential to all data being kept and saved on our servers. The password policy is extended from the new user up to our corporate offices. It is important to remember the value of our data and the trust we instill in our clients. |

|  |
| --- |
| 3.2 Acceptable Use Policies One of the big challenges that comes with protecting the users that work for the company is to enable employees to be able to work at their best, while at the same time maintain a strong security standard for the information technology network, and most importantly the information that is held within that data.  Any system that is being used, should only be used for work purposes, so this includes allowing users to use things like social media accounts, or other websites that are not related to work, and when talking about systems that means all the IT equipment that would be connected to our corporate network, or would access anything applications that the corporation uses, this would include desktops, laptops, smartphones, tablets, printers, data and voice networks, software, as well as electronically-stored data, portable storage devices (I.E. hard drives, USB) and anything else that would be covered by this term.  All users that are on the network should only be doing their work on the company’s systems. All data on the system is the property of the company Cyberleet, and all users within the company should be told that at any time the company can view their system and view its content.  We want to enforce the rule that users are not to do any personal business on the company’s system, is because we monitor all use on the systems within the company, and if a user’s personal information were to put on to the system, people in the security department, and if any leaks were to occur, that information could then be stolen. |

|  |
| --- |
| 3.3 User Training Policies Here at Cyberleet, we want to be definite that all employees are trained and acknowledge the policies in place. Every employee will sign off on a quarterly acknowledgment whether new or senior to the company. Each employee should understand the principles and abide by the training methods given to them. The company's foundation is critical and every role in the company matters. Training will be conducted annually as a refresher and each employee will endorse their attendance of the annual training. Within the company, each team may foresee different modules of training based on roles granted to them. Each department level may share a different responsibility and the proper training is important to the staff functioning within their respective departments. Cyberleet will focus on innovative ways to keep every employee up to date and highlight how each department plays a critical role that platforms the company's foundation. |

|  |
| --- |
| 3.4 Basic User Policies The policies set in place is the responsibilities of each employee. By agreeing to these terms there are required steps that must be acknowledged and taken to ensure that the company is secured at the user's level. The password policy will make sure that the company's computer systems are secured and prevent any duplication of employee sign-on. This will extend out to deterrent any form of unauthorized access. Once the employee endorses their agreement to the company’s policies, every guideline should be followed in to which each employee will hold responsibility for their safekeeping of their computer station. This is critical and essential that every user understands the measures of every action made by them will not hinder any unauthorized access of any kind. In addition to the password policy, granted access will be controlled in which the user will be able to access data or company information. This will extend out to company property as well, as certain employees may hold special access dependent on the roles granted to them. Each user will gain access based on the sole roles of each individual that pertains to their job responsibilities and the title they hold. Additional access will be granted by the proper authorities by approval from upper management, promotional status, or job deadlines. Every user will be allowed to access the internet for the main purpose of conducting business for the organization. Any personal use of any kind is prohibited and will fall under a misconduct of company property. The restrictions use will include but are not limited to, political use of side business, political solicitations, any form of harassment, and offensive materials related to any inappropriate level. In addition to these restrictions, Each user may not use computing and networking resources for any illegal or unauthorized activities. which include the following:  · Online Streaming  · Social Media (if not authorized)  · harassing statements  · Downloading unapproved software/games  · Emailing classified information to another source of any kind.  . Gambling     Every employee should understand these acceptable use and policies in place. It would be suggested that every user accepts the companies policies upon login on acceptable use set in place by the systems administration. Approving and accepting to gain entry each user should understand the roles and purpose of proper use of each computer system. Each employee will acknowledge and stamp there sign on digitally before access is granted into the main network. This procedure will ensure and remind that each user understands the integrity of the organization and is a reminder of the purpose we serve as an employee. This policy will also be extended to new hires that will acknowledge there understanding of this policy. |

A threat-intelligence service provides analyzed, actionable threat information to help organizations defend against known or emerging threats before systems may be compromised. In this section, you will create three mitigation scenarios. The first two mitigation topics have been chosen; however, the third one is your choice. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

# SECTION 4: Threat Mitigation Scenarios

|  |
| --- |
| 4.1 Theft  Physical security is critical for cyberleet, There are three main things that should be minded: detection, prevention, and recovery. Prevention is a critical cause it makes the organizations network a target for breaches. Most hackers take or opportunities that are easy to breach. The companies platform should not possess any weak points to avoid these issues. In case of any breaches within the company, detection ensures the company to respond in a critical matter. There are many detection tools that Cyberleet has and any minor or major alarms should never go unseen. A Recovery is set in place to deal with the breach at hand. It factors and ensures the proper departments to review and overlook the overall security levels in place to determine where what, and how the breach occurred. To harden any and every security peripherals set in place. We want to design a physical security perimeter. This will prevent unauthorized visitors from accessing the building which is crucial not only for the safety of the business but the employees as well.   All Physical entry points to the building must be protected and the hindrance methods would be in place. A combination of deterrents would include a steel perimeter gate, proper lighting at a high lumen, ID checkpoints/card readers, and a turnstile with a CCTV camera. By Utilizing a steel gate around the perimeters of the buildings along with CCTV cameras, staff will be accounted for and time stamps could be logged by review. This will keep unauthorized personnel entering the company grounds. Adding proper lighting within the parking lot and the external building will ensure that visibility is not questionable during after-hours. With the use of CCTV cameras, it will allow video surveillance in the event of any matter. All CCTV system reviewing. An external drive would be allocated to keep footage at least a minimum of six months for tracking purposes.        As additional security measures, all users will be signed a CAC/Badge for entry into the company premises. A turnstile will use to allocate a front and back entry which would have a CCTV camera as an additional layer of security. Each member ID will come with an RFID chip issued by the company which will serve as a log and time stamp upon entry. The ID method will serve as a double authentication method. Each badge will grant access to the user's perspective areas which will limit personal from roaming into unauthorized areas. In addition to every member on board, company property will only be available to employees unless permitted by the right authorities within the company. Upper management will log and track any visitation to ensure that every event is accounted for. Employees who require remote access via VPN or RAP to continue to work outside the company are determined by upper-management and reasoning would play a big factor in granting that privilege. Remote access should only be approved to meet deadlines and complete special projects. The ability to obtain remote access will be limited and not offer to every member of the organization. |

|  |
| --- |
| 4.2 Malware To prevent any malware from infecting any of our systems in place, below you will find key guidelines that should be followed.   * Ensure all operating systems and platforms are up to date to its standards. * Keep all internet browsers up to date with latest versions and patches available. * Enable anti-virus scanning of all e-mails as a barrier for any unwanted mail or viruses. * Install proper anti-virus software’s, anti-spyware, anti-rootkit, and personal firewalls alongside encryption keys to safeguard the systems. * Use updated pop-up blockers to prevent adware. * Preform scanning frequently of the network, to look for any types of malware.   Train employees of awareness of any possible threats and unknown sources. |

|  |
| --- |
| 4.3 Your Choice **Scenario:**  An employee in the IT department has been using his knowledge of the network to steal, and sell information from the company to its competitors, as well as hackers.   * Perform background checks on all employees that will have access to sensitive material before being hired by the company. * When new employees are boarded into the company, Access should be limited to any computer systems until the employee is vetted and onboard completely. * Train employees on account protection and make sure they understand they are responsible for their own identity. * Monitor every employee’s actions when he or she is logged into a system. * Educate employees on the rules that have been created by the IT department and have them endorse an agreement to ensure they understand what is expected of them. * Use a two-step authentication method to make sure that it is the user logging in. * Use refresher courses to keep all employees up to date with the company's policies set in place. |

# SECTION 5: References

|  |
| --- |
| *Prompt: If applicable, list all references used in the creation of this document here. References must be in APA format.* |

##### **What Is Availability? - Definition from Techopedia**https://www.techopedia.com/definition/990/availability

##### **Information Security** <https://en.wikipedia.org/wiki/Information_security>

##### **Confidentiality, Integrity and Availability**

Amir - <https://devqa.io/confidentiality-integrity-availability/> OCT 2019