Organization Logo (Optional)

Log Management Policy

Organization Name

Date

Created by: CYBERSAFE SQUAD

**** CYBERSAFE SQUAD HAS DEVELOPED THIS FILLABLE TEMPLATE AS PART OF THE CYBERSECURE BLUEPRINT PROCESS FOR EDUCATIONAL PURPOSES ONLY. THIS TEMPLATE IS INTENDED TO PROVIDE GUIDANCE ON HOW TO ORGANIZE AND DOCUMENT INFORMATION FOR LOG MANAGEMENT POLICIES. PLEASE NOTE THAT THE USE OF THIS TEMPLATE DOES NOT GUARANTEE SUCCESSFUL CERTIFICATION OR COMPLIANCE WITH ANY REGULATORY REQUIREMENTS. ORGANIZATIONS ARE NOT OBLIGATED TO USE THIS TEMPLATE AND MAY CHOOSE TO PROVIDE CERTIFICATION REQUIREMENTS IN A FORMAT THAT BEST SUITS THEIR NEEDS AND REQUIREMENTS. ****

Index

Instructions for Using the Template

Here are the instructions on how to fill this template.

This fillable template is intended to assist users in meeting the certification requirements for the Computer Security Log Management security control area for Cybersecure Process.

- Red font instructions are provided within each section of the template. These should be deleted upon completion of the template.
- Tables are included for instructional purposes only and should be deleted upon completion of the template.
- We recommend that users review the eLearning module for Computer Security Log Management and the completed example of this policy to ensure understanding and accuracy.

Context of the Log Management Policy

- A log is a record of activities in an organization's systems and networks, containing information related to specific activities.
- Logs are generated by various sources, including security software, operating systems, and applications.
- Log management is crucial to store computer security records in detail for an appropriate period.
- Regular log analysis helps identify security incidents, policy violations, fraudulent activity, and operational problems.
- Logs aid in auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying trends and long-term issues.

Definitions of Key Terms

1. Activity: An occurrence within a system or network that triggers a response, such as changes to a firewall configuration or user logins.

2. Log Entry: Information recorded in response to an activity, such as time stamps, user IDs, IP addresses, and system events.

3. Log: A record of all activities and events occurring within an organization's systems and networks, including security alerts, error messages, and user activity logs.

4. Log Management: The process of generating, transmitting, storing, analysing, and disposing of log data to ensure the security and reliability of the system and network.

5. Log Analysis: The process of studying log entries to identify significant events, trends, and patterns that may indicate security threats or operational issues.

6. Log Rotation: The process of closing a log file and opening a new one when the first log file is considered complete, to ensure the continuity of logging.

7. Resting State: The state of log files when they have been transferred to a log storage solution and are no longer being actively updated.

8. Transmission State: The process of moving log files from individual assets to the log storage solution, such as a centralized logging server or cloud-based logging service.

9. Availability: The ability to access the right information or systems when required by authorized individuals, such as IT administrators or security analysts.

10. Confidentiality: The protection of sensitive information from unauthorized access, such as personal data, financial information, and business secrets.

11. Integrity: The protection of information from unauthorized modification, deletion, or corruption, to ensure the accuracy and reliability of log data.

Revision History of the Policy

Regular review and updating of policies is crucial for organizations to ensure that their practices align with their goals and comply with legal requirements. In addition, keeping a record of policy changes can help organizations track the evolution of their policies over time, and ensure that employees are aware of and comply with the most recent versions of policies.

It is recommended that organizations:

- Conduct regular reviews of their policies to ensure they are up-to-date and effective.
- Identify specific individuals or teams responsible for policy development and implementation, as well as for reviewing and updating policies.
- Develop clear guidelines for documenting policy changes, including the name of the person responsible for making the changes, the date of the change, the rationale for the change, and any relevant details about the change.
- Ensure that all employees are aware of policy changes and that they receive training or communication regarding any updates.
- Maintain a record of all policy changes, along with the date of the change, the individual responsible, and any relevant details. This record can be used to demonstrate compliance with legal or regulatory requirements, as well as to evaluate the effectiveness of policy changes over time.

Date	Version	Modification	Modifier
[Date edited]	[Document version]	[Description of changes made]	[Name of the editor]

The date for the next scheduled review of the Log Management policy: DD-MMM-YYYY

Scope of the Policy

Scope Statement:

- Insert the scope statement that outlines the boundaries and objectives of the policy.

Responsibilities:

- Identify the person or team who will be responsible for overseeing and executing the policy.
- The responsible individual or team should have a clear understanding of the scope statement and be equipped with the necessary resources and authority to effectively implement the policy.
- The responsibilities may include developing and communicating the policy to relevant stakeholders, monitoring compliance, conducting regular reviews and updates, and addressing any issues or concerns that arise.
- It is essential to ensure that the responsible individual or team is accountable for the success of the policy implementation and has a well-defined plan for carrying out their responsibilities.

The following policy is applicable to the designated [Name/Team] responsible for implementing and managing a robust log management system at [Organization Name]. The policy aims to outline the key areas of focus for establishing an effective log management system. These areas include:

- Roles and Responsibilities: This section will define the roles and responsibilities of the personnel involved in the log management system, including the designated team, the users, and any other stakeholders.
- Log Sources: The policy will identify the sources of logs that need to be monitored, tracked, and analyzed. These logs may include servers, applications, network devices, and other relevant sources.
- Rules for Logging: This section will lay out the guidelines and standards for logging data, such as what data should be logged, how frequently data should be logged, and what format should be used.
- Log Analysis: The policy will outline the procedures for analyzing and interpreting the logged data, such as tools and techniques used for analyzing the logs and the frequency of analysis.
- Log Security: This section will define the measures taken to ensure the security and integrity of the logs, such as access controls, encryption, and backup and recovery procedures.

The policy is designed to ensure that the log management system is efficient, effective, and secure in achieving the organizational goals and objectives.

Roles and Responsibilities of Personnel Involved

In order to ensure effective log management, it is crucial for an organization to establish a clear framework for assigning roles and responsibilities to individuals and teams involved in this process. By doing so, the organization can streamline its log management planning process and improve the overall security of its systems and data.

To help organizations achieve this goal, the following types of activities and responsibilities should be considered when defining roles and responsibilities:

- Identification of individuals and teams responsible for log collection, analysis, and retention
- Specification of the types of logs to be collected and the methods for their collection
- Designation of individuals responsible for log analysis and response to security incidents
- Establishment of protocols for regular log review and analysis to identify potential security threats or breaches
- Definition of the methods for log retention and archiving, including the length of time logs will be stored
- Identification of individuals responsible for managing access to log data and ensuring its confidentiality and integrity

By outlining these activities and responsibilities in a comprehensive policy document, organizations can create a clear and effective log management plan that will help to protect their systems and data from potential security threats.

The individuals listed will be responsible for various tasks related to log management. These responsibilities may include:

• Configuring log sources to ensure that all necessary data is being captured accurately.

• Analyzing logs to identify any potentially suspicious activities or security threats.

• Initiating responses to any identified activities to minimize the risk of a security breach.

• Managing log storage to ensure that logs are stored securely and can be easily accessed if needed.

• Monitoring the logging status of all log sources to ensure that logs are being generated as expected.

• Checking for upgrades and patches to logging software if applicable, and acquiring, testing, and deploying them.

• Ensuring that each logging host’s clock is synchronized to a common time source to ensure consistency across all logs.

• Reconfiguring logging as needed based on policy changes, technology changes, and other factors to ensure optimal performance and security.

• Documenting and reporting any anomalies in log settings, configurations, or processes.

For smaller organizations, some of these responsibilities may be fulfilled by the same team member. In general, team and individual roles involved in log management may include the following:

• Log analyst: responsible for analyzing logs to identify security threats and other anomalies.

• Log manager: responsible for managing log storage, monitoring logging status, and ensuring that logging is configured correctly.

• Security analyst: responsible for overall security of the organization, including log management.

• IT administrator: responsible for managing the IT infrastructure, including logging software and other tools.

• Compliance officer: responsible for ensuring that the organization is in compliance with all relevant regulations and standards, including those related to log management.

It's crucial to ensure that log management is performed efficiently and effectively to maintain the security and compliance of the organization. Therefore, assigning clear roles and responsibilities to individuals and teams is necessary to achieve this goal.

Name (s)	Position	Role	Contact
	Chief information officers (CIO)	This role includes the following responsibilities: overseeing the IT resources that generate, transmit, and store the logs	
[Insert Name(s)]	System and network administrators	This role includes the following responsibilities: • Configuring logging on organization assets, • analyzing logs, • reporting on the results of log management activities, and • performing regular maintenance of the logs and logging software	[Insert Contact Info]
[Insert Name(s)]	Security administrators	This role includes the following responsibilities: • managing and monitoring the log management system, • configuring logging on security devices (e.g., firewalls, network based intrusion detection systems, antivirus servers), • reporting on the results of log management activities, and assisting others with configuring logging and performing log analysis	[Insert Contact Info]
[Insert Name(s)]	Computer security incident response team	This role (which is more thoroughly detailed in your Incident Response Plan) includes the following responsibilities: • fulfilling the incident response procedures detailed in [Organization Name]'s Incident Response Plan using log data when handling incidents in compliance with [Organization Name]'s policy	[Insert Contact Info]

[Insert Name(s)]	Procurement Officers	This role includes the following responsibilities: • purchasing of software that should or can generate computer security log data. ***This role may include many other responsibilities related to procurement however for this policy the role is specifically relating to the procurement of software.*	[Insert Contact Info]
[Insert Name(s)]	Application developers	This role includes the following responsibilities: designing or customizing applications so that they perform logging in accordance with the logging requirements and recommendations	[Insert Contact Info]
[Insert Name(s)]	Auditors	This role includes the following responsibilities: using log data when performing audits	[Insert Contact Info]

When will the Log Management policy be reviewed next?

**In many large organizations, log management is typically not fully centralized. Instead, it is distributed among different teams, such as system administrators, network administrators, and security administrators. Each team is responsible for managing logging on their systems, analyzing their log data on a regular basis, documenting and reporting the results of their log management activities, and ensuring that log data is provided to the person(s) responsible for the entire log management system according to the policy.

However, smaller organizations may choose to perform all log management centrally, rather than on individual systems. This is often the case when there are not multiple teams managing different systems, and one person manages the entire IT infrastructure for the business. Alternatively, the organization's infrastructure may not be complex enough to require a more distributed approach to log management.

In summary, some key points to note regarding log management in organizations include:

• Log management is often not fully centralized in larger organizations. • In larger organizations, different teams are responsible for log management on their systems. • Regular analysis of log data is important for effective log management. • Log management activities should be documented and reported in accordance with policy. • Smaller organizations may choose to perform all log management centrally.

Log Sources to Be Monitored

List of Hardware and Software Assets

Organizations are required to identify all their hardware and software assets that can perform activities that are loggable based on their specific needs. The list of such assets can be found in Figure 1 under the "Asset" column. Once the assets are identified, the organizations need to determine which activities they should log for each of their in-scope hardware and software systems. If the organization has already developed a Digital Asset Catalogue (DAC) as part of the Automatically Patch Operating Systems and Applications Module, they can use it to identify in-scope and out-of-scope assets for their log management system. Alternatively, the organization can conduct an inventory of its hardware and software assets to identify which ones are in-scope and out-of-scope for logging purposes.

Asset	Activity	Log Entry	Log File Name	Storage Location	Log Frequency	Impact Level	Log Retention	Date Created
Firewall	Config changes	Username of Account	FWConfig Logs	D:\LogStorage\FW	Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Configuration Change			Every occurrence			Nov 11, 2021
	Rule changes	Username of Account	FWRules Logs		Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Rule Change			Every occurrence			Nov 11, 2021
	User logins	Username of Account	FWUsers Logs		Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Successful/Failed Attempts			Every occurrence			Nov 11, 2021

Activities and Log Entries to Be Recorded

- In order to effectively log activities for each hardware and software asset in an organization, the following steps should be taken:

- Determine which activities must or should be logged for each asset.
- Based on the identified activities, determine the types of log entries that should be captured.
- Note that multiple logs can be generated from the same source, such as a firewall.
- Organizations must decide which types of activities they want to be logged, such as configuration changes, rule changes, and user logins.
- From the logged activities, the organization must determine which types of log entries from each activity they want or need to be logged.
- For example, a configuration activity on a firewall may require various types of log entries, including the username of the account that performed the activity, the IP address of the user, the time and date of the activity, and the actual configuration change that occurred.
- Overall, a clear understanding of the activities to be logged and the types of log entries required is crucial for effective logging and monitoring of an organization's assets.

Asset		Log Entry	Log File Name	Storage Location	Log Frequency	Impact Level	Log Retention	Date Created
Firewall	**Config changes**	**Username of Account**	FWConfigLogs	D:\LogStorage\FW	Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Configuration Change			Every occurrence			Nov 11, 2021
	Rule changes	**Username of Account**	FWRulesLogs		Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Rule Change			Every occurrence			Nov 11, 2021
	User logins	**Username of Account**	FWUsersLogs		Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Successful/Failed Attempts			Every occurrence			Nov 11, 2021

Rules for Logging

Some potential rules for logging frequency, retention, rotation, and analysis based on an organization's determination of low, moderate, and high-impact systems:

For Low-Impact Systems:

- Logging Frequency: Log at least once a day or when changes are made to the system
- Log Retention Period: Keep logs for 30 days or until they reach a size limit of 100 MB
- Log Sizes and Rotation: Rotate logs when they reach 100 MB or weekly, whichever comes first

For Moderate-Impact Systems:

- Logging Frequency: Log at least once an hour or when changes are made to the system
- Log Retention Period: Keep logs for 60 days or until they reach a size limit of 500 MB
- Log Sizes and Rotation: Rotate logs when they reach 500 MB or daily, whichever comes first

For High-Impact Systems:

- Logging Frequency: Log every few minutes or when changes are made to the system
- Log Retention Period: Keep logs for at least 6 months or until they reach a size limit of 1 GB
- Log Sizes and Rotation: Rotate logs when they reach 1 GB or hourly, whichever comes first

It's important to note that these rules are just examples, and organizations should determine their own logging rules based on their specific needs and the potential impact of a compromise to their systems. Factors to consider when defining logging settings include the frequency and severity of threats faced, the potential impact on the CIA triad, and the storage available to the organization.

	Low-Impact System	Moderate-Impact System	High-Impact System
Retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
Rotate logs	Every week or every 25 MB	Every 6 to 24 hours or every 2 to 5 MB	Every 15 to 60 minutes or every 0.5 to 1 MB
Analyze log data	Every 1 to 7 days	Every 12 to 24 hours	At least every 2 hours

- The CIA triad is a risk management model that focuses on the three essential aspects of information security.
- Availability is one of the key elements in the CIA triad, referring to the ability of authorized personnel to access required information or systems.
- Confidentiality is another crucial component of the CIA triad, emphasizing the need to safeguard sensitive information from unauthorized access.
- Integrity is the third pillar of the CIA triad, highlighting the importance of protecting information from unauthorized modification or deletion.

Example:
company has three types of systems: low-impact systems (such as printers and basic desktop computers), moderate-impact systems (such as servers and databases), and high-impact systems (such as financial systems and critical infrastructure).The company determines that for their low-impact systems, they will log at least once a day or when changes are made to the system, retain logs for 30 days or until they reach a size limit of 100 MB, and rotate logs when they reach 100 MB or weekly, whichever comes first. For their moderate-impact systems, they decide to log at least once an hour or when changes are made to the system, retain logs for 60 days or until they reach a size limit of 500 MB, and rotate logs when they reach 500 MB or daily, whichever comes first. Finally, for their high-impact systems, they determine that they need to log every few minutes or when changes are made to the system, retain logs for at least 6 months or until they reach a size limit of 1 GB, and rotate logs when they reach 1 GB or hourly, whichever comes first. These logging rules are based on the potential impact of a compromise to each system, with high-impact systems requiring more frequent and detailed logging and longer retention periods. The specific logging settings may vary depending on the needs and available resources of each organization.

Frequency of Logging

- Evaluate the specific requirements of each asset and activity before deciding on the frequency of logging.
- Consider factors such as the criticality of the asset, regulatory compliance requirements, and storage capacity available when determining the appropriate logging frequency.
- Examples of common logging frequencies include logging every occurrence, once for all instances in x minutes, once for every X instance, and every instance after x instances.
- For the asset 'firewall' and the activity 'configuration changes', logging every occurrence is recommended.
- For the asset 'printer' and the activity 'printed documents', logging the details once for every X instance is suggested to optimize storage capacity.
- When logging every occurrence, record relevant details such as the username of the account, IP address, time and date, and the configuration change for each activity.
- When logging once for every X instance, record relevant details such as the username of the account, IP address, time and date, and the number of pages for each activity.
- Align the logging frequency with the specific needs of the business to ensure effective risk management and compliance.

Asset		Log Entry	Log File Name	Storage Location	Encrypted	Log Frequency	Impact Level	Log Retention	Date Created
Firewall	**Config changes**	**Username of Account**	FWConfigLogs	D:\LogStorage\FW	Yes	**Every occurrence**	**High**	1 year	Nov 11, 2021
		IP Address				**Every occurrence**			Nov 11, 2021
		Time and Date				**Every occurrence**			Nov 11, 2021
		Configuration Change				**Every occurrence**			Nov 11, 2021
	Rule changes	Username of Account	FWRulesLogs			Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address				Every occurrence			Nov 11, 2021
		Time and Date				Every occurrence			Nov 11, 2021
		Rule Change				Every occurrence			Nov 11, 2021
	User logins	Username of Account	FWUsersLogs			Every occurrence	**High**	1 year	Nov 11, 2021
		IP Address				Every occurrence			Nov 11, 2021
		Time and Date				Every occurrence			Nov 11, 2021
		Successful/Failed Attempts				Every occurrence			Nov 11, 2021
Printer	Config changes	Username of Account	Printer Config Logs	D:\LogStorage\Printer	No	Every occurrence	Moderate	6 months	Jan 28, 2021
		IP Address				Every occurrence			Jan 28, 2021
		Time and Date				Every occurrence			Jan 28, 2021
		Configuration Change				Every occurrence			Jan 28, 2021
	Printed docs	**Username of Account**	Printer DocsLogs			**Once for every file printed**		6 months	Jan 28, 2021
		IP Address				**Once for every file printed**			Jan 28, 2021
		Time and Date				**Once for every file printed**			Jan 28, 2021
		Number of pages printed				**Once for every file printed**			Jan 28, 2021

Retention Period of Log Data

Asset		Log Entry	Log File Name	Storage Location	Encrypted	Log Frequency	Impact Level	Log Retention	Date Created
Firewall	**Config changes**	**Username of Account**	FWConfigLogs	D:\LogStorage\FW	Yes	Every occurrence	High	**1 year**	Nov 11, 2021
		IP Address				Every occurrence			Nov 11, 2021
		Time and Date				Every occurrence			Nov 11, 2021
		Configuration Change				Every occurrence			Nov 11, 2021
Printer	**Config changes**	**Username of Account**	Printer Config Logs	D:\LogStorage\Printer	No	Every occurrence	High	**6 months**	Jan 28, 2021
		IP Address				Every occurrence			Jan 28, 2021
		Time and Date				Every occurrence			Jan 28, 2021
		Number of Pages				Every occurrence			Jan 28, 2021

In order to maintain effective cybersecurity and protect against potential threats or breaches, it's essential for businesses to implement an appropriate log retention policy. The length of time that logs are retained will depend on a number of factors, including the impact level of each system, the activity being logged, and the log entries for each activity. By taking these factors into account, businesses can determine the appropriate retention period for their logs, ensuring that they are available for analysis and investigation when necessary.

As previously discussed, certain systems may have a higher impact on a business if compromised. This impact level can help to determine the appropriate log retention period, as logs for these systems may need to be retained for a longer period of time. It's important to define these retention settings based on the specific needs of your business, taking into account factors such as regulatory compliance requirements, legal obligations, and risk management considerations. Additionally, the storage available to your organization will also play a role in determining the appropriate log retention period, as businesses will need to ensure that they have sufficient storage capacity to retain logs for the required time period.

Overall, implementing an appropriate log retention policy is an important aspect of maintaining effective cybersecurity. By taking into account the impact level of each system, the activity being logged, and the available storage, businesses can define retention settings that align with their specific needs and help to protect against potential security threats.

Log Rotation Procedures

The size of logs plays a critical role in determining the effectiveness of a business's logging system. Several factors influence the size of logs, including the number of assets that require logging, the frequency of logging, and the log retention period. The larger the logs, the more frequently they need to be rotated to preserve log entries and prevent the file size from becoming too large to manage. Proper log rotation helps ensure that log data is accessible, searchable, and usable, allowing organizations to quickly identify security incidents and address them before they escalate.

Log rotation frequency is another essential factor that impacts the management of log data. Log rotation frequency determines how often a log file is closed and a new file is created based on either a schedule or a specific file size. The primary benefit of log rotation is that it helps to preserve log entries while preventing the file size from becoming unmanageable. Once a log file is closed, it can be compressed to save storage space, making it easier to store and manage a large volume of log data. By implementing an effective log rotation policy, organizations can maintain the integrity of their log data, improve their security posture, and respond quickly to potential security incidents.

Log Analysis Procedures

- Regular log analysis is crucial for identifying security incidents, policy violations, fraudulent activity, and operational problems, as well as for supporting internal investigations, establishing baselines, and identifying trends and long-term issues.
- It is the responsibility of a specified individual or team to ensure that log files are regularly analyzed to detect any anomalies.
- The analysis of log files can be performed either manually or through the use of software.
- For each system listed in the assets column of this policy for [Organization Name], a manual analysis of the log files is to be performed, with the frequency of log analysis based on the impact level of each system.
- [Organization Name] utilizes a designated log analysis software for all log analysis requirements, and it is the responsibility of the specified individual or team to ensure that any upgrades and patches to the logging software are obtained, tested, and deployed as soon as they are available.

• [Name/Team/Individual] is accountable for regularly examining log files to identify any irregularities. [Organization Name] employs _____ log analysis for this purpose.

• [Name/Team] is responsible for acquiring, testing, and implementing upgrades and patches for logging software as they become available.

• A manual examination of the log files is conducted on every system listed under the assets column of this policy for [Organization Name].

• The frequency of log analysis is determined by the impact level of each system.

	Low-Impact System	**Moderate-Impact System**	**High-Impact System**
Retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
Rotate logs	Every week or every 25 MB	Every 6 to 24 hours or every 2 to 5 MB	Every 15 to 60 minutes or every 0.5 to 1 MB
Analyze log data	**Every 1 to 7 days**	**Every 12 to 24 hours**	**At least every 2 hours**

Prioritization of Log Entries

Organizations can prioritize which log entries to analyze by considering various factors. These factors include the type of entry, whether it's new or recurring, the source of the log, and the IP address of the source or destination. Additionally, they can also consider the time of day or day of the week when the entry occurs, and how frequently it occurs within a certain period.

In simpler terms, organizations can prioritize which logs to analyze based on various factors such as the type of log, where it came from, and when it happened. They can also consider whether the log is new or recurring and how often it occurs. By doing so, they can quickly identify and address potential issues that could impact their systems' security and functionality.

Response to Identified Activities

If an unusual event related to cybersecurity is detected, it is crucial for the organization to respond quickly and effectively. To do so, it is recommended to have an incident response plan in place that outlines the necessary steps to be taken. This plan should cover key questions such as what to do when an anomaly is detected, who to report it to, and how to document the incident. It is important to follow the procedures outlined in the incident response plan to ensure that the issue is addressed appropriately.

To put it simply, if your organization detects any suspicious activity related to cybersecurity, it is important to have a plan in place to respond to it. This plan should include steps on what to do when an anomaly is detected, who to report it to, and how to document the incident. Following the procedures outlined in the incident response plan is important to ensure that the situation is handled appropriately. The Cyber Shield Blueprint offers guidance on developing an incident response plan, which can be a helpful resource for organizations.

Measures for Ensuring Log Security

To keep your business's log files safe, it's important to take some precautions. Firstly, limit access to the log files to only those who need to create entries. Even then, they should only have append-only privileges and no read access if possible. They should also not be able to perform any operations on log files, such as renaming or deleting them. Secondly, avoid logging sensitive data that isn't necessary, such as passwords. If possible, only log required information that doesn't pose a risk if accessed by unauthorized people. Lastly, protect stored log files by encrypting them and physically securing them. However, not all logs need to be encrypted, so it's important to determine which logs require this level of protection based on your business's needs.

In simpler terms, logs are records that contain information about what happens on your business's computer systems. To keep these records safe, you should limit who can access them and what information is logged. Only those who need to add information to the logs should have permission to do so. Sensitive information, like passwords, should be kept out of the logs whenever possible. Finally, log files should be kept secure by encrypting them and storing them in a safe location. It's important to remember that not all logs need to be encrypted, so you should determine which ones require this level of protection based on your business's needs.

It is the duty of [Name/Team] to ensure that log files are secured suitably and satisfactorily, in accordance with the data contained in each log, for the benefit of [Organization Name]. Employing the best industry practices, it is advisable to encrypt all log files in both storage and transmission states.

If applicable include the following statements regarding your businesses encryption and log storage:

The log files of [Organization Name] are subject to encryption, utilizing [specify encryption type], to ensure their confidentiality. Moreover, said log files are kept in a secure location. Additionally, the transmission of [Organization Name]'s log files is encrypted, using [specify encryption type], for added protection.

Guidelines for Accessing Log Files

When it comes to securing your organization's logs, it's important to think about who needs to access the log data and how that access should be monitored. Here are a few things to consider when creating your access policy:

- Keep a record of all log accesses so you can monitor who is looking at the data.
- Limit who can read the log data and regularly review those privileges to ensure only the necessary people have access.
- Prevent users from making changes to log files, including deleting or renaming them.
- Generally, users should not have access to log files unless they need to create log entries. In those cases, they should only be given append-only privileges and no read access if possible.

In summary, it's important to have a clear and monitored policy in place for accessing log data. By limiting who can read the logs and preventing users from making changes, you can help ensure the integrity of your organization's data.

The management of log file data at [Organization Name] falls under the purview of [Name/Team] to guarantee that access to log files remains regulated.

Insert any other statement(s) regarding your organizations log file access policies.

Enforcement of the Log Management Policy

The policy mandates that [Name/Team] is accountable for supervising the log management procedures outlined in this document.

Asset	Activity	Log Entry	Log File Name	Storage Location	Log Frequency	Impact Level	Log Retention	Date Created
Firewall	Config changes	Username of Account	FWConfigLogs	D:\LogStorage\FW	Every occurrence	High	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Configuration Change			Every occurrence			Nov 11, 2021
	Rule changes	Username of Account	FWRulesLogs		Every occurrence	High	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Rule Change			Every occurrence			Nov 11, 2021
	User logins	Username of Account	FWUsersLogs		Every occurrence	High	1 year	Nov 11, 2021
		IP Address			Every occurrence			Nov 11, 2021
		Time and Date			Every occurrence			Nov 11, 2021
		Successful/Failed Attempts			Every occurrence			Nov 11, 2021
VPN Software	Config changes	Username of Account	VPNConfigLogs	D:\LogStorage\VPN	Every occurrence	High	1 year	Oct 5, 2020
		IP Address			Every occurrence			Oct 5, 2020
		Time and Date			Every occurrence			Oct 5, 2020
		Configuration Change			Every occurrence			Oct 5, 2020
	User logins	Username of Account	VPNUserLogs		Every occurrence	High	1 year	Oct 5, 2020
		IP Address			Every occurrence			Oct 5, 2020
		Time and Date			Every occurrence			Oct 5, 2020
		Successful/Failed Attempts			Every occurrence			Oct 5, 2020
Printer	Config changes	Username of Account	PrinterConfigLogs	D:\LogStorage\Printer	Every occurrence	Moderate	6 months	Jan 28, 2021
		IP Address			Every occurrence			Jan 28, 2021
		Time and Date			Every occurrence			Jan 28, 2021
		Configuration Change			Every occurrence			Jan 28, 2021
	Printed docs	Username of Account	PrinterDocsLogs		Once for every unique file	Moderate	6 months	Jan 28, 2021
		IP Address			Once for every unique file			Jan 28, 2021
		Time and Date			Once for every unique file			Jan 28, 2021

		Number of pages printed			Once for every unique file			Jan 28, 2021
Payroll Software	User Logins	Username of Account	PayrollLogins	D:\LogStorage\Payroll	Every occurrence	High	1 year	March 25, 2020
		IP Address			Every occurrence			March 25, 2020
		Time and Date			Every occurrence			March 25, 2020
		Successful/Failed Attempts			Every occurrence			March 25, 2020
	Config Changes	Username of Account	PayrollConfig Logs		Every occurrence	High	1 year	March 25, 2020
		IP Address			Every occurrence			March 25, 2020
		Time and Date			Every occurrence			March 25, 2020
		Configuration Change			Every occurrence			March 25, 2020
	Software Updates	Username of Account	PayrollUpdate Logs		Every occurrence	High	1 year	March 25, 2020
		IP Address			Every occurrence			March 25, 2020
		Time and Date			Every occurrence			March 25, 2020
		Software update			Every occurrence			March 25, 2020