A black background with a black square

Description automatically generated with medium confidence

Security

Student Name: Raneem Yahya Sa’deh

Student ID: 22210016

Instructor Name: Eng. Sami Al-Mashaqbeh / Eng. Elham Derbas

­

Course Name: Security

HTU Course No: 00203280

BTEC Unit No: D/618/7406

Academic Year Fall 2023/2024

A grey logo on a black background

Description automatically generated with low confidence

Contents

[**Introduction** 3](#_Toc157442535)

[**Risk Assessment** 4](#_Toc157442536)

[A. ISO 31000 4](#_Toc157442537)

[ISO 31000 framework and guidelines 4](#_Toc157442538)

[ISO 31000 Principles: 6](#_Toc157442539)

[ISO 31000 Process: 7](#_Toc157442540)

[B. Controls Initially 7](#_Toc157442541)

[C. Possible Risks 8](#_Toc157442542)

[CyberBlast Crispy system's possible risks 10](#_Toc157442543)

[D. Suggested Controls 14](#_Toc157442544)

[E. Evaluating 15](#_Toc157442545)

[F. Data Protection Processes 17](#_Toc157442546)

[**Security Policy** 18](#_Toc157442547)

[Introduction 18](#_Toc157442548)

[A. CyberBlast Crispy Security 18](#_Toc157442549)

[1. Security Policy 18](#_Toc157442550)

[2. Disaster Recovery Plan 18](#_Toc157442551)

[B. Security Plan 20](#_Toc157442552)

[C. Evaluating: 25](#_Toc157442553)

[D. Misalignment 26](#_Toc157442554)

[**Security Auditing** 28](#_Toc157442555)

[A. IT Security Auditing 28](#_Toc157442556)

[B. Stakeholders Roles 29](#_Toc157442557)

[**CEO Presentation** 31](#_Toc157442558)

[1. Possible Risks 31](#_Toc157442559)

[2. Improperly Configuring Network 31](#_Toc157442560)

[3. Network Security Techniques 31](#_Toc157442561)

[4. Network Monitoring System 32](#_Toc157442562)

[5. Physical and Virtual Security Measures 33](#_Toc157442563)

[**Appendix** 34](#_Toc157442564)

[**REFERENCES** 43](#_Toc157442565)

**A group of food on a table

Description automatically generated**

# **Introduction**

In the landscape of the culinary realm, CyberBlast Crispy Company stands as a prominent player, offering delectable and irresistibly crispy fried chicken. Despite our recent estaplishment, our venture has swiftly ascended to prominence, becoming a preferred choice for individuals and connoisseurs seeking an indulgent and flavorful culinary experience. At CyberBlast Crispy Company, our commitment goes beyond our delicious fried chicken; it encompasses the integration of innovation and technology into our operations.

Embracing cutting-edge IT infrastructure, we have meticulously designed our systems to ensure not only the efficiency of our operations but also the secure handling of data in accordance with industry standards. Our commitment to utilizing technology underpins our culinary artistry, ensuring that every mouthful of our crispy chicken not only pleases the palate but also embodies our unwavering devotion to the highest caliber standards. The purpose of this report is to analyze the cybersecurity measures employed by CyberBlast Crispy Company, evaluate their robustness, and propose enhancements to enhance our commitment to secure and technologically driven culinary excellence. By implementing these suggestions, our goal is to elevate CyberBlast Crispy Company's standing, establishing it as a pioneer in delivering not just delicious but also technologically secure fried chicken offerings.

# **Risk Assessment**

## ISO 31000

162 national standards bodies are members of the **International Organization for Standardization**, an independent non-governmental organization. Through its members, ISO brings professionals together to exchange ideas and create voluntary, consensus-based, internationally applicable standards that foster innovation and address global issues. Over **22,000** international standards and related papers covering nearly every area that uses standards, including technology, healthcare, agriculture, and food safety, have been produced by ISO.

The long-term success of an organization depends on many things, from constantly updating and evaluating its offerings, and this will improve its operations. Also, they need to consider the unexpected in risk management. That's why the **ISO 31000** for risk management was developed, and its last version was released in 2018, and it was designed for any organization seeking clear guidance on risk management.

**What is ISO 31000 Risk Management?**

ISO 31000 Risk Management: What Is It**?**

Organization for Standardization (ISO) established the ISO 31000 Risk Management framework. It is applicable to all businesses, regardless of kind, size, activity, or location, and offers them guidelines and principles for risk management. It includes every kind of risk. It was created by a variety of stakeholders and is meant to be used by all risk managers, not just experts.

### ISO 31000 framework and guidelines

It is a set of steps and actions that support the risk management system throughout the facility.

We have six distinct areas:

* **Leadership:** Leaders in the organization must take responsibility to make sure ISO 31000 is adopted and applied in a way that aligns with the company's goals and culture.
* **Integration:** Risk management should be integrated at all levels of the organization and in all processes because it's important not to cause operational bottlenecks or stand in the way of core business processes being performed.
* **Design:** The organizations need to design strategy for the risk management based on their needs. For example, the key drivers and trends affecting the objectives of the organization.
* **Implementation:** The implementation process integrates the organization's risk management design into business processes, such as developing an appropriate plan including time and resources. And his plan can be developed in the future if needed.
* **Evaluation:** Evaluation looks at the design to see what is working and what might need to be refined.
* **Improvement:** Organizations should continuously look for ways to improve their ISO 31000 implementation, to address external and internal changes in doing. So, the organization can improve its value.

### ISO 31000 Principles:

Effective risk management requires the elements of the image below and can be further explained as follows.

A diagram of value creation and protection

Description automatically generatedWe have seven polices:

* **Inclusive:** To be able to take knowledge and perspective into consideration, stakeholders need to provide relevant input at the right time, which will lead to improving awareness and informed risk management.
* **Dynamic:** Risks can emerge both externally and internally within the organization suddenly. Therefore, risk management anticipates, explores, and responds to them.
* **Best available information:** risk management’s inputs are based on the current and past information, as well as on the predicted information. So, this information must be clear for relevant stakeholders.
* **Human and cultural factors:** The impact of humans on risk management is significant at every stage and level.
* **Continual improvement:** The risk management must be continually improved through experience and knowledge.
* **Integrated:** To be integrated in the or organization operations.
* **Structured:** The structured approach will help to consistent and comparable results for the risk management.
* **Customized:** To be proportionate to the organization’s external and internal context a framework is customized for risk management.

### ISO 31000 Process:

Here are the six processes:

* **Risk identification:** now the obstacles that might stop us from reaching our goals at organizations.
* **Risk analysis:** What are the threats that have been discovered in the organization sources and causes.
* **Risk evaluation:** Evaluating the residual risk's reasonableness by contrasting the findings of the risk analysis with the risk standards.
* **Risk treatment:** Changing the negative and positive likelihood of consequences of organization, to achieve a net grow in benefit.
* **Establishing the context:** This activity includes defining the scope of the risk management process, the organization's goals, and the criteria for evaluating risks. The context is made up of internal (organizational governance, culture) and external (market conditions, stakeholder expectations) elements.
* **Monitoring and review:** This task compare both indicators in organizations and risk management performance to make sure that they are fully reviewed, and they check that they have not deviated from the plan and that organizations private policy fits the plan.

**Communication and consultation:** To communicate with the stakeholders and understand their interests and be sure that the risk management is focusing on the correct points.

## Controls Initially

The organization's assets face several threats and vulnerabilities, each requiring specific controls to mitigate the risks. Devices (endpoints) are vulnerable to hacking because of a lack of anti-malware software and intrusion detection systems. Expired firewall licenses, unrestricted access to HR and finance devices, and the lack of a DMZ deployment compromise network security. To address this, the network is divided into public and internal subnets.

Data and client personal information are at risk because of insecure web transmision and weak hashing algorithms. Existing controls include improving the hashing algorithm. Backups stored in a public cloud without encryption pose a threat to secrecy, integrity, and availability, but there are routine backups and SSL/TLS protocols during the transmission.

The web server uses a vulnerable OpenSSH version with a high critical vulnerability score. And there are no controls in place to address this issue. Employees face phishing. The data center lacks physical security and environmental control, affecting confidentiality, avalability, and integrity, with no existing controls.

Expired VPN encryption and unrestricted third-party VPN access jeopardize user and employee data. No controls exist due to an expired digital certificate. Data security risks involve employees using others' login credentials, affecting confidentiality, avalability, and integrity. Cameras and paper\_cutting tools serve as limited controls to prevent changes or deletions.

Various systems, servers, databases, and the firewall face risks due to a misconfigured firewall and weak credential protection including inadequate password policies and a lack of physical security policies, impacting confidentiality, availability, and integrity. Currently, there are no existing controls to address these policy issues.

## Possible Risks

**Risk Likelihood**

|  |  |  |
| --- | --- | --- |
| **Rating** | **Likelihood Description** | **Expanded Definition** |
| 1 | **Rare** | May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely. |
| 2 | **Unlikely** | Could occur at some time but not expected given current controls, circumstances, and recent events. |
| 3 | **Possible** | Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences. |
| 4 | **Likely** | Will probably occur in some circumstance, and one should not be surprised if it occurred. |
| 5 | **Almost Certain** | Is expected to occur in most circumstances and certainly sooner or later. |

**Risk Consequences**

|  |  |  |
| --- | --- | --- |
| **Rating** | **Consequence** | **Expanded Definition** |
| 1 | **Insignificant** | Generally, a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization. |
| 2 | **Minor** | Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency. |
| 3 | **Moderate** | Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event. |
| 4 | **Major** | Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off. |
| 5 | **Catastrophic** | Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely. |
| 6 | **Doomsday** | Multiple instances of major systemic security breaches. Impact duration cannot be determined, and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management are expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely. |

**Risk Level Determination and Meaning**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Consequences** | | | | | |
| **Likelihood** | **Doomsday** | **Catastrophic** | **Major** | **Moderate** | **Minor** | **Insignificant** |
| **Almost Certain** | E | E | E | E | H | H |
| **Likely** | E | E | E | H | H | M |
| **Possible** | E | E | E | H | M | L |
| **Unlikely** | E | E | H | M | L | L |
| **Rare** | E | H | H | M | L | L |

|  |  |
| --- | --- |
| **Risk Level** | **Description** |
| **Extreme (E)** | Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts. |
| **High (H)** | Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls is likely to be met from within existing resources. |
| **Medium (M)** | Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews. |
| **Low (L)** | Can be managed through routine procedures. |

### CyberBlast Crispy system's possible risks

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Num. | Asset | Threat/ Vulnerability | Existing Controls | Likelihood | Consequence  (Impact) | Level of Risk |
| *1* | Devices (endpoints) | Lack of anti-malware software and the host-based intrusion detection system.  Then anyone can hack these devices and he might see and edit and delete the data.  will affect on the C, A, and I. | The security team works diligently, but their efforts can sometimes be hindered by employees who don't cooperate and disabling the portable storage on end devices to protect against malware spreading. | Likely | Doomsday | Extreme |
| *2* | Network | Expired firewall licenses, HR, and Finance device accessibility, no DMZ deployment, it will effect on the C, A, I because the guest can see the data on the HR and Finance device and edit and delete it. | Dividing the network into public and internal | Almost Certain | Major | Extreme |
| *3* | Data, Client personal information | Data is transmitted through an insecure web, Using a Usage weak hashing algorithm.  This data could be seen so it will effect on the C, also it could be changed by the attackers and this will effect on the I and A | Weak hashing algorithm | Almost Certain | Doomsday | Extreme |
| *4* | Backups data | one of these backups is stored in a public cloud without encryption.  This data could be seen so it will effect on the C, also it could be changed by the attackers and this will effect on the I and A | Routinely backups, using SSL/TLS protocols only during the transmitting and SHA1 hashing algorithm | Likely | Major | Extreme |
| *5* | Web server | Use of vulnerable OpenSSH version which has a maximum score of 9.8/10 that shows a big critical vulnerability. This critical OpenSSH vulnerability would allow attackers to gain unauthorized access to data, by changing or deleting or seeing it. It will affect on C, A, I | There is no existing control | Almost Certain | Catastrophic | Extreme |
| *6* | Employee | phishing email and ransomware attachment.  If the employee opens the file there might be a virous so this will effect on the C, A, and I. | There is no existing control, but fortunately, the employee didn't open the attachment | Unlikely | Moderate | Medium |
| *7* | Data center | Lack of physical security and security mechanisms, bad environmental control.  will effect on the C, A, and I. | No Existing Controls | Almost Certain | Doomsday | Extreme |
| *8* | User and employee’s data | VPN encryption has been expired and Unrestricted third-party VPN access | No Existing Controls because the digital certificate used for VPN encryption is expired. | Likely | Major | Extreme |
| *9* | Data | Employee who uses others login credentials can see, change, and delete the data so that will affect on the C, A, and I. But for the camera and the printed data people can only see the data without changing it or deleting it, so what will affect only on the C. | Cameras, scissors for cutting paper. | Possible | Moderate | (High) All this happens in the same company so the risk will not be very high but if the printed data has been troughed outside the company any one can see this data. |
| *10* | various systems, servers, databases, and the firewall | C: See the data, A: Change the data, I: Delete the data,  misconfigured firewall, the essential credentials protection is very weak | Firewall With misconfiguration, very weak password | Almost Certain | Doomsday | Extreme |
| *11* | The CyberBlast Crispy company (policy) | policy issues, inadequate password policy in terms of length, complexity, and hashing for the database, no physical security policies. will effect on the C, A, and I. | No Existing Controls | Almost Certain | Catastrophic | Extreme |

**Notes:  
SHA-1:** SHA-1 was once considered a secure hash algorithm; it is now vulnerable to various attacks. (Not secure)

**SSL/TLS protocol:** TLS is an updated, more secure version of SSL, and TLS is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers.

**C, I, A**: **C** stands for Confidentiality, **I** stands for Integrity, **A** stands for Availability.

## Suggested Controls

|  |  |
| --- | --- |
| Critical Asset | Suggested Controls |
| Devices (Endpoints) | Use anti-malware applications and software, host-based intrusion detection systems (HIDS), and prevent installation of unauthorized programs.  Apply strong policies for the security assessment. |
| Network | Implement DMZ to make isolation between the application and the database server, Make strict access controls for Finance and HR devices.  Renew firewall licenses.  intrusion detection systems (IDS) and intrusion prevention systems (IPS) |
| Data, Client personal information | Use a strong hash algorithm such as SHA-256, Ensure that the data is transmitted securely. |
| Web server | Patch and update OpenSSH.  intrusion detection systems (IDS) and intrusion prevention systems (IPS) |
| Data center | Monitoring the environment, implementing strict policies to enable access, uninterruptible power supply (UPS). |
| Various systems, servers, databases, and the firewall | Install the latest firewalls.  intrusion detection systems (IDS) and intrusion prevention systems (IPS) |
| The CyberBlast Crispy Policy | intrusion detection systems (IDS) and intrusion prevention systems (IPS), Apply a strong policy in the company. |

## Evaluating

A risk assessment is a systematic process performed by a competent person that involves identifying, analyzing, and controlling hazards and risks present in a situation or place. The purpose of this decision-making tool is to identify the necessary measures for controlling or eliminating risks and to prioritize them based on their likelihood and impact on the business.

Risk assessment is one of the major components of a risk analysis. The process of risk analysis consists of several steps that seek to identify and analyze all risks and issues that could harm a business or enterprise. This is a constantly developing process that is updated as needed. These ideas are linked and have individual uses.

|  |  |
| --- | --- |
| Security Risk Assessment Approach | A combined approach using baseline and detailed risk analysis |
| Acceptable Risk Level | Low  CyberBlast Crispy's risk management strategy is consistent with industry practice by setting a low, acceptable level of risk. This demonstrates that the company is active and caution in protecting its assets and customer data and availability of its IT infrastructure and services. |
| Risk Assessment Type | Qualitative |
| Risk Assessment Process | 1. I studied the organization and by collecting information about it I could **understand the system**, its assets, and the existing controls. 2. I identify the **assets** in CyberBlast Crispy Company. 3. I link the **existing controls** to the recognized assets, establishing the connection between protective measures and vital components. 4. Define **vulnerabilities and threats** that have the potential to affect the identified critical assets. 5. Assess the **likelihood** of each identified risk that threatens the company, depending on the steps above, leveraging a combined approach that integrates detailed and baseline analysis methodologies. This assessment is also informed by my experience in the security field. 6. I also determined the **impact** of each risk on the company's assets, I considered the type of threat and the importance of the critical asset involved. 7. Depending on the impact and likelihood of the risk on the critical assets in the company, I could know the risk **level** (Extreme, High, Medium, and Low), and this provided a comprehensive understanding of the potential threats. 8. Based on the things I found from all these steps, I will give **recommendations** for controls and countermeasures that aim to strengthen the assets in the company and mitigate the identified risks effectively. |

**Different between Qualitative and Quantitative:**

The choice between quantitative and qualitative risk assessments depends on the criteria, such as the organization's nature, the specific objectives of the risk assessment, and the resources that are available. Both have advantages and disadvantages. Here are some reasons why quantitative is considered better:

* Qualitative risk assessments typically use subjective descriptions and assessments. It may lack the precision of quantitative data. It may be difficult to evaluate and compare risks effectively, while quantitative risk assessments involve numerical values for risks, which enable accurate assessment and comparison and allow organizations to rank risks according to likelihood and possible impact.
* Qualitative risk assessments don't have detailed cost-benefit analysis because it lacks financial granularity and might not offer the data required to make choices based on financial considerations, while quantitative risk assessments allow cost-benefit analysis, helps in calculating the return on investment for security measures, and gives businesses a clear awareness of prospective losses, enabling them to make financial decisions.
* Qualitative risk assessment prioritization is usually based on subjective judgments, and risks' relative importance might not be as clear. It might be challenging to find out which risks pose the greatest threat to the organization, while quantitative risk assessment allows risk to be systematically prioritized using a numerical scale. This helps to concentrate resources on the risks that have the greatest potential to affect the organization.

## Data Protection Processes

Within its dynamic culinary ecosystem, CyberBlast Crispy Company prioritizes data protection. To maintain a strong data protection framework, CyberBlast Crispy follows some processes and regulations. In a world where data holds critical insights into our operations, accomplishments, clients, and user's experiences, it's important to protect this information from potential harm, unauthorized access, or alterations, notably aligning with the principles embodied in the General Data Protection Regulation (GDPR).

Data protection in CyberBlast Crispy includes:

**Designing the system** and emphasizing privacy and security to make sure that all the sensitive data stays confidential and secure.

While processing data, **stringent security measures** are in place to protect data during the processing step, preventing unwanted access and capture.

Data processing should comply with several **legal grounds**, such as contracts, permission, public tasks, legitimate interests, vital interests, or legal obligations.

While transmitting the data, we should use **encryption and hashing algorithms** to make sure that the data is secure, maintain data integrity, and thwart unauthorized access.

**Regularly backup** the data to create accurate copies, acting as a safeguard against data modification or deletion.

Using a very strong **anti-malware application** serves as a preventive measure against unauthorized access and potential data breaches.

Using **firewall protection** to filter out malicious actions on the network fortifies the IT infrastructure against cyber threats.

**Analysis, logging, and monitoring** of the data to swiftly identify and prevent potentially harmful data transfers.

Getting **rid** of sensitive data that is no longer needed, whether physical or digital.

Always check the devices that store data and ensure they are carefully **maintained** to prevent corruption or inaccessibility issues.

To make sure that the sensitive data is transferred securely, we use **VPNs**.

Employees are **taught about attacks** during regular security awareness training sessions, which helps them identify and block possible risks.

# **Security Policy**

## Introduction

A written document outlining an organization's information technology (IT) and physical asset protection procedures. Security policies are dynamic documents that are updated and modified regularly in response to changes in technology, security requirements, and vulnerabilities.

Are **security policies** important?

It protects the assets, both physical and digital, of the organization and identifies all threats to those assets.

Physical security policies include:

Sensitive rooms, buildings, and other regions inside an organization who is authorized to move, handle, and access physical assets; protocols and other guidelines for handling, monitoring, and gaining access to these assets; and the accountability of persons regarding the physical assets they handle and access.

The importance of **maintaining security standards:**

To make sure that the confidential data are safety, comply with regulations, earn customer loyalty, mitigate dangers, and preserve operational stability, security standards must be upheld. This demands a holistic strategy that includes periodic security evaluations, staff education, technology upgrades, and constant surveillance to cope with changing risks and weaknesses.

## CyberBlast Crispy Security

### Security Policy

[*The policy is attached in the appendix.*](#_Policies)

### Disaster Recovery Plan

CyberBlast Crispy Disaster Recovery Policy

**1. Overview:**

Despite the rarity of disasters, CyberBlast Crispy recognizes that being ready with a thorough disaster recovery (DR) plan can mean the difference between disruption and resilience. This policy explains the value of funding DR initiatives and requires the creation and execution of a strong plan to guarante prompt recovery from unanticipated events affecting our IT systems and operations.

**2. Purpose:**

In the case of any significant outage, regardless of the reason, this policy mandates the creation of a CyberBlast Crispy-specific disaster recovery plan that covers the recovery of vital IT systems, programs, and data.

**3. Scope:**

This policy describes the high-level need for the DR plan's existence but does not go into depth about its precise contents or sab-plans; it applies to all CyberBlast Crispy IT workers who oversee creating, testing, and maintaining the plan.

**4. Policy:**

**4.1 Contingency Plans:**

The development and integration of the following essential contingency plans is required for the overall disaster recovery plan: Cybersecurity Incident Response Plan: This plan outlines roles, responsibilities, and procedures for prompt response and mitigation in the event of cyberattacks or security breaches; Business Continuity Plan: This plan identifies critical business functions, prioritizes their restoration, and describes temporary workarounds to minimize operational disruption during recovery; Data Backup and Recovery Plan: This plan specifies data types, backup schedules, storage locations, and recovery procedures to ensure timely data restoration in the event of loss; System and Infrastructure Recovery Plan: This plan describes the steps involved in restoring essential IT systems and infrastructure, including prioritization, dependencies, and equipment replacement.

**4.2 Testing and Maintenance:**

To find and fix any vulnerabilities, the DR plan needs to be tested frequently using table-top exercises and simulations. Every year, the plan should be revised to account for changes in risks, systems, and infrastructure.

**5. Policy Compliance:**

The information security team will use a variety of techniques, such as audits, reviews, and feedback channels, to keep an eye on compliance.

**6. Exceptions and Consequences:**

The InfoSec team must grant permission in advance for any exceptions to thispolicy, and noncompleance may result in disciplenary action.

* **The Main Components**

A **DRP** team can offer invaluable insights and expertise that can help the organization recover from a disaster more effectively. In addition, a DRP team can assist the organization in identifying and mitigating the risks asociated with its disaster recovery plan. This team oversees developing and executing the disaster recovery plan, and it should be composed of people with experience in a variety of fields, including IT, business continuity, and emergency management.

It is important that the recovery time objective (**RTO**) be realistic, achievable, and based on the impact of the disruption on the business in order to guarante that systems and data are recovered within a specified timeframe. This is particularly crucial for businesses that depend on their systems to operate. By incorporaeting RTO into the organization's disaster recovery plan, the business can be certain that its systems will be operational in the event of an emergency.

Recovery point objectives (**RPO**) are the maximum amount of data that can be lost in a disaster. They should be determined by the business's acceptable level of data loss. RPOs can help prevent data loss, guarantee timely data recovery, enhance the overall effecteveness of the disaster recovery process, and make sure that the organization's disaster recovery plan complies with all applicable regulations.

**Backups** are crucial for data recovery following a disaster. They should be kept in a secure location, like a waterproof and fireproof safe, and should be tested regularly. Backups can help ensure that data is accessible in the event of a system failure, which is another reason they are important. Finally, backups can shorten the time it takes for data recovery following a disaster.

A well-**documented** disaster recovery plan makes it easier to follow in the event of a disaster. It should include procedures for all aspects of the plan, including data backup and recovery, system failover, and communication. It also acts as a roadmap for how the plan will be carried out; without it, it may not work as intended or be incorrectly followed. Documentation also makes it possible to review and revise the plan as needed, which is important to keeping it current and useful.

**Automation** can be used for tasks like data backup, standby system failover, and notification sending. Automation can help to speed up the process of recovering from a disaster, ensure that all necessary steps are taken to recover from the disaster, and reduce the amount of human error that can occur during the disaster recovery process. Automation can help to reduce the time and effort required to impliment the disaster recovery plan.

## Security Plan

*Remote Access Security Plan*

**Policy Overview:**

* Goal: The main goal of the Remote Access Security policy is to establish secure and controlled access to the organization's network from external locations. And our plan aims to ensure the secrecy, integrity, and availability of important data by implementing strong measures for remote connections.

**Authentication and Access Control:**

User Authentication: Implement strong user authentication mechanisms that will help to verify the identity of users who are accessing the network remotely.

Access Control: Enforce strict access controls to limit remote access privileges for only the authorized employees and users.

**Encryption and Data Integrity:**

Use encryption protocols for remote connections to protect the secrecy and integrity of the transmitted data.

Secure Protocols: Enforce the use of secure communication protocols, such as VPNs for remote access.

**Device Security:**

Make sure that devices used for remote access follow the security standards and have updated antivirus software.

Put in place protocols to verify and validate remote devices before allowing them to connect to the network.

**Logging and Monitoring:**

Enable complete logging of remote access activities to track user actions and catch any suspicious behavior.

And this monitoring of remote access activities must be in real time, to identify and respond promptly to potential security incidents.

**Multi-Factor Authentication (MFA):**

Encourage the use of multi-factor authentication for remote access to add an extra layer of security.

**Follow the policies:**

Making sure that the users are accessing the network remotely follow the organization's security policies, including password policies and aceptable use policies.

**User Education and Awareness:**

Make regular training sessions to educate users on secure remote access practices, threats, and the importance of maintaining the confidentiality of data.

**Incident Response:**

Develop an incident response plan specific to remote access security incidents and put a procedare for promptly reporting any suspected security incidents related to remote access.

**Enforcement and Consequences:**

Clearly communicate the conseqences for non-compliance with the remote access policy, including temporary suspension of access privileges and define a process for reporting and addressing policy violations related to remote access promptly.

**Timetable:**

Month 1-4: Develop and communicate the new Remote Access Security Plan.

Month 5-6: Implement technical changes to enforce policy requirements for remote access.

regularly: periodic reviews and updates to the Remote Access Security Plan as needed.

**Maintenance:**

Make sure to regularly review and update the Remote Access Security Plan to match the latest industry standards and additional security risks.

Also, collect feedback from users and IT support related to remote access to address any challenges or concerns.

*Internal Servers Security Plan*

**Policy Overview:**

Goal: The principal goal of the internal server security policy is to make secure practices for accessing and managing sensitive data stored within CyberBlast Crispy Company's internal servers. This plan aims to ensure the confidentiality, integrity, and availabilty of important information.

**Authentication and Access Control:**

User Authentication: Implement robust user authentication mechanisms to make sure that only authorized users can access internal servers.

Access Control: enforce strict access controls to limit server access to individuals with specific job roles and responsibilities.

**Password Management:**

Apply regular password changes, for example, every 70 days, to mitigate the risk of compromised credentials for internal servers.

Password History: Implement a password history policy to prevent users from reusing their last passwords for internal servers.

Set an account lockout policy for internal servers to disable accounts temporarily after a specified number of unsucessful login attempts, discouraging brute-force attacks.

**User Education and Awareness:**

Training: Train the users regularly about the importance of accessing internal servers, educating them on recognizing and reporting potential security threats.

Security Guidelines: Put clear guidelines on secure device usage, especially for internal servers, informing users about the risks asociated with unauthorized software installation.

**Multi-Factor Authentication (MFA):**

Enable MFA: Encourage or mandate the use of multi-factor authentication for accessing internal servers to add an extra layer of security.

**Password Storage and Transmission:**

Ensure that passwords for internal servers are stored and transmitted securely using industry-standard encryption protocols.

Hashing: Implement password hashing techniques to protect stored passwords for internal servers in case of a data breach.

**Password Recovery:**

Establish a secure and verifiable password recovery process for internal servers that involves multi-step authentication to prevent unauthorized access.

**Accountability:**

User Responsibility: Clearly communicate that users are responsible for safeguarding their passwords for internal servers and prompt reporting of any suspicious activities.

Administrative Access: Limit administrative access to internal servers to only those individuals who require it for their job functions.

**Monitoring and Auditing:**

Conduct audits of user accounts and passwords for internal servers to identify and address security vulnerabilties.

Log password-related events for internal servers and regularly review logs for any anomalies.

**Enforcement and Consequences:**

Policy Enforcement: Clearly state the repercussions of failing to adhere to internal server security measures. There are potential consiquences, such as temporary restrictions on device usage or even suspension of network access.

User Accountability: Emphasize user responsibility in safeguarding their devices with access to internal servers and adhering to security policies.

**Timetable:**

Month 1–4: Develop and communicate the policy.

Month 6–8: Implement technical changes to enforce policy requirements for internal servers.

Ongoing: Doings periodic reviews and updates to the policy as needed.

**Maintenance:**

Regularly review and update the policy to stay current with new threats and industry best practices.

And, Gather input from users and IT support to address any issues or concerns related to internal server security.

*User Account Credentials (Password) Security Plan*

**Policy Overview:**

Goal: The main goal of the User Account Credintials Security Plan is to establish secure practices for managing and protecting user passwords. This plan aims to ensure the confidential natureconfidentiality, integrity, and availability of user accounts across the organization.

**Password Creation and Complexity:**

To enhance complexety and resistance to brute-force attacks, it is recommended to set a minimum password length of 12 characters. Strong and secure passwords can be created by mandating the use of a combination of uppercase and lowercase letters, numbers, and special characters. To minimize the risk of compromised credentials, it is advisable to enforce regular password changes, for example every 70 days. Additionally, implementing a password history policy can prevent users from reusing their last passwords. To discourage brute-force attacks, consider setting an account lockout policy to temporarily disable accounts after a specified number of unsuccessful login attempts.

**User Education and Awareness:**

Regularly make security awareness training sessions to educate users on the importance of strong passwords, potential threats, and best practices for safeguarding their account credentials, and provide clear guidelines on creating secure passwords, and inform users about the risks asociated with weak or easily guessable passwords.

**Multi-Factor Authentication (MFA):**

strongly recommend the implementation of multi-factor authentication for all user accounts on every system and application to enhance security measures.

**Password Storage and Transmission:**

Make sure that the passwords are stored and transmitted securely using industry-standard encryption protocols.

Also, Implement password hashing techniques to protect stored passwords in case of a data breach.

**Password Recovery:**

Secure Process: Establish a secure and verifiable password recovery process for user accounts that involves multi-step authentication to prevent unauthorized access.

**Accountability:**

User Responsibility: Clearly communicate that users are responsible for safeguarding their passwords and prompt reporting of any suspicious activities.

Administrative Access: Limit administrative access to user account cridentials to only those individuals who require it for their job functions.

**Monitoring and Auditing:**

Regular Audits: Conduct periodic audits of user accounts and passwords across all systems and applications to identify and address security vulnerabilities.

Log password-related events and regularly review logs for any anomalie.

**Enforcement and Consequences:**

Enforcement: Establish consequences for non-compliance with the User Account Credentials policy, including temporary account suspension or access restriction

Reporting Violations: Define a process for reporting and addressing policy violations related to user account credentials promptly.

**Timetable:**

Month 1-2: Develop and communicate the new policy.

Month 3-4: Implement technical changes to enforce policy requirements for user account credintials.

Ongoing: Do periodic reviews and updates to the policy as needed.

**Maintenance:**

Regular Updates: Regularly review and update the policy to align with industry best practices and emerging security threats.

User Feedback: Collect feedback from users and IT support to address any challenges or concerns related to user account credintials and security.

## Evaluating:

|  |  |
| --- | --- |
| Tools used within the policy | The Evaluation of the Tool |
| VPN | Implementing a Virtual Private Network (VPN) makes the data transmission more secure by encrypting communication channels. This saves sensitive information from potential eavesdroping and makes sure that the connection between different network locations is secure. Thus, adding an extra layer of protection against potential unauthorized access and threats. |
| Password | Utilizing strong password policies is essential for access control. Putting a policy to use a complex password requirements and regular password updates enhances the overall security posture, and that's reduces the risk of unauthorezed access to systems and accounts. |
| Encryption | Make sure that the sensitive data is protected by implementing encryption techniques that will add extra layer of protection. By encoding information in a way that only allowed parties can decipher encryption safeguards against unauthorized access, protecting the confidentiality and integrity of critical information. |
| Servers | The policy includes making sure the servers have regular maintenance, and the security of servers, patching, and monitoring. These servers contribute to a robust infrastructure, minimizing vulnerabilities and potential points of exploitation that could compromise the overall network security, so this will enhance the overall integrity and availability of organizational data and services. |
| Access control | Implementing access control systems restricts user access based on their roles and responsibilities. This prevents unauthorized individuals from accessing sensitive resources and enhances the overall security of the organization's systems and data, such as the cards and fingerprint unlocks. |

## Misalignment

**Remote Access Policy Misalignment:**

Unauthorized or insecure remote access could cause data breaches, compromise of sensitive information, and potential harm to the company's reputation.

So, you have to make sure that all remote access connections adhere to the Remote Access Policy's guidelines, including the use of encryption technologes, strong passwords, and compliance with approval and security measures. regularly review and update the policy to address emerging threats.

**VPN Policy Misalignment:**

Weak VPN configurations may causes unauthorized access, data interception, or compromised confidentiality during remote access.

Align VPN configurations with the VPN Policy, emphasizing user responsibility for managing VPN services securely. And regularly update VPN gateways, apply strong authentication measures, and monitor compliance to prevent security vulnerabilities.

**Server Security Policy Misalignment:**

Weak server configurations may expose vulnerabilities, leading to unauthorized access or data breaches.

Make sure that serves adhere to the Server Security Policy by implementing approved configurations, promptly applying security patches, and maintaining proper change management. regularly monitor and log security-related events to detect and respond to potential threats.

**Password Protection Policy Misalignment:**

Weak passwords will cause to unauthorized access, identity theft, or compromise of sensitive information.

Apply the Password Protection Policy by promoting strong password creation, secure handling, and regular updates. Learn users on password security best practices and consider implementing multi-factor authentecation for privileged accounts.

**Acceptable Encryption Policy Misalignment:**

Failing to comply with encryption standards can result in insecure communication, data breaches, or legal and regulatory repercussions.

Make sure encryption practices are in line with the Acceptable Encryption Policy, which includes using approved algorithms, managing keys properly, and following industry standards. It is important to consistently assess and upgrade encryption technologes to proactively address ever-changing security risks.

**Maintaining Alignment**

To ensure continuous alignment between IT security and CyberBlast Crispy's policy:

Make regular security assessments and audits.

Make sure to update security policies regularly to stay current with emerging threats and industry standards.

Foster a security-aware culture through training the employees in all departments of the company.

Set up a dedicated security team to monitor and respond to security incidents.

Apply a continuous improvement process for security policies and practices.

Making sure that employees and executives read and understand the policy and follow it without exception.

By maintaining these policies, CyberBlast Crispy can enhance its IT security measures, alegn them with the established policy, and better safeguard its assets, data, and overall business operations.

# **Security Auditing**

## IT Security Auditing

The IT security audit conducted on CyberBlast Crispy Company's infrastructure has identified critical vulnerabilties across various areas, including physical components, applications and software, network vulnerabilities, and human. These weaknesses are a significant threat to the company's overall security, potentially leading to reputational damage, financial losses, and compromised user safety.

**Analysis**

**Physical Components:**

* Lacking physical security measures leaves the company vulnerable to unauthorized access, risking sensitive data and information.
* The data center's security weakness, such as easily accessible doors and the fact that there are no security cameras or access logs, created potential risks, including server malfunctions and data loss.
* Device security is lacking, allowing open access for employes, and weak security passwords pose a significant vulnerability.

**Application and Software:**

* The issues with the firewall and VPN undermine the security of the software, making data and information easy to access.
* Insuficient security measures in the software create significant vulnerabilities, increasing the risk of security breaches.

**Network Vulnerabilities:**

* A critical vulnerability exists in the network, like lack of segmentation, missing DMZ, insecure HR and Finance access, and expired firewall licenses, that will compromise network security.

**Human Dimensions:**

* Insufficient training for the employees on security threats and data protection poses a significant risk to the organization.

**Security Audit Impact:**

The identified IT security flaws have severe implications for CyberBlast Crispy Company.

* Lack of physical protection increases the risk of unauthorized access to hardware, potentially compromising data processing and resulting in financial losses.
* Weak security software, irregular updates, and helpless security policies create exploitable vulnerabilities that pose a serious threat.
* Non-encryption of stored and transferred data facilitates easy access for attackers, risking exposure of sensitive information.
* Insufficient employee awareness increases vulnerability to common attacks.
* lack of accountability leaves the company susceptible to financial consequences without assigning responsibility for the loss of assets.

**Solving these problems:**

* Using strong physical security measures, including data center access controls, cameras, badges, and environmental controls.
* Enhance device security by implementing stronger password policies.
* Address configuration issues with firewalls and VPN to ensure robust software-level security.
* Implement encryption protocols for data in transit to safeguard against unauthorized access.
* Conduct regular employee training programs to enhance awareness of security threats.
* Put accountability measures to identify and address security incidents promptly.

**Future Implications for Security Measures:**

Handle these vulnerabilities is crucial for CyberBlast Crispy Company to fortify its security measures and maintain the trust of its stakeholders. Our company should prioritize these recommendations in its security roadmap to create a resilent and secure IT environment for its critical assets.

## Stakeholders Roles

Many stakeholders, from management to employees with varying responsibilities, must collaborate in order to guarantee that the company's security is established and that it is shielding the organization from the effects that the risks would cause if the risks materialize. Each of these stakeholders has a part to play in the recommendations and execution of the security audit.

**Here is how different stakeholders affect the security audit:**

**Management**

**CEO:**

* Promote the establishment of a security-oriented culture and actively advocate for the implementation of security initiatives.
* Give the needed resources to ensure the effectiveness of security measures.
* Accept the security policies and plans proposed by the CISO and the security team.

**Department Heads:**

* Apply security policies within their respective departments.
* Ensure that employees under their management receive proper security training.

**IT Personnel**

**CISO:**

* Manage all the security strategies and policies.
* Evaluate and decrease risks across all systems and networks.
* Lead incident response in cases of security breaches.

**IT Security Manager:**

* - Implement security policies that are consistent with the company's objectives.
* - Manage the security team and make sure that they are trained well and aware of security best practices.
* - Make regular security assessments and audits to identify vulnerabilities and gaps.
* - Manage and develop disaster recovery and incident response plans.

**End-Users**

**Regular Employees:**

* - Follow the company's security policies and procedures in their work.
* - Use strong passwords and don't share their login credentials.
* - Inform the IT department immediately of any suspicious activities or security incidents.

**Risk Owners**

* They work with the management section and IT personel in order to check that the risks identified in the security audit are mitigated and that the system is less likely to be threatened.

**Security Officers**

* They make sure that the premise is secure against any physical access. They most importantly is to make sure that the on-premise data center is secure and that no unathorized access to it has been made.

**Compliance Officers**

* They make sure that the organization and the rest of the employees and managers from all the section are compliant to the security audit recommendations and there is no misalignment is happening.

# **CEO Presentation**

## Possible Risks

1. Devices (End points)
2. Network
3. Various systems, Servers, Databases, And Firewall
4. Data center
5. The CyberBlast Crispy company (policy)

## Improperly Configuring Network

It could cause a different type of cyberattacks, such as data theft, ransomware attacks, denial-of-service attacks, and malware infections.

This mis-configured system helps Cybercriminals to steal sensitive data, gain unauthorized access, or disrupt business operations.

Firewalls:

Improper Configuration: Allowing to much traffic through the firewalls and put the setting of the firewall in the default that might not give the adequate protection. And don’t update the firewall regularly.

Exploitation Consequences: This misconfiguration can cause unauthorized access to the network. It will help the attackers to exploit compromise sensitive and vulnerabilities and denial-of-service (DoS) attacks.

Recommended Actions: Update the firewall regularly, analyze the actions happens in the firewall for suspicious activity. The manufacturer should use more layers in security and make a combination between the firewall and the IDS and IPS as will it is in the NGFW.

Third-party VPNs:

Improper Configuration: Using easily guessable or default credentials, using outdated versions from TLS or SSL can cause a security vulnerability in the VPN.

Not updating or patching the VPN regularly

Exploitation Consequences: The data will be accessed unauthorized, and the traffic will be intercepted.

Recommended Actions: Using strong encryption and regularly update and patch the VPN, educating about the policies that the employees should follow because that will enhance the security posture of the organization.

## Network Security Techniques

DMZ (Demilitarized Zone):

Explanation: It's a type of Network architecture that divide the company's network from the remainder of its infrastructure to provide a layer of security, The main purpose from it to isolate the internal network from the public one because it has sensitive and important data and information.

Effectiveness: It works as a firewall, it will isolate your network from others to hack it, it controls the traffic flow and determines which data can be shown outside.

Static IP (Internet Protocol):

Explanation: It's unchangeable address it is assigned to a device, during the sessions of the network the static IP doesn't change or refresh, it helps to monitor the network traffic and control the network.

Effectiveness: Distant and controlled device access. Helps in better control and monitoring of network traffic.

NAT (Network Address Translation):

Explanation: Agent between the local and the public network, so many devices are represented as a single IP address outside their networks, NAT allows single devices like the router to make this.

Effectiveness: It does effectively manage the limit of IPv4 address space, could access to the internet in widespread.

Challenges: There are some applications that connect directly (end-to-end), which will disrupt NAT.

If your device were behind more than one NAT (at work, home, or university), that will complicate communication.

## Network Monitoring System

The NMS surveils the devices, systems, and network traffic in real-time. And this will enable the unusual behavior or security threats in the network to be detected, like abnormal data traffic patterns or unauthorized access attempts and identify the security incidents such as unusual data transfers, network intrusions, or malware outbreaks rapidly.

SNMP (Simple Network Management Protocol):

is an application layer protocol that gives managers and agents a message format for communication. It also enables network administrators to monitor and manage the performance of their IP networks, identify and fix network issues, and plan for future network expansion. End devices managed by network administrators include servers, workstations, routers, switches, and security appliances.

NetFlow:

Cisco IOS technology provides statistics on packets passing through the router or multilayer switch. It can track byte and packet counts for that specific application flow, monitoring application connections, and it can provide data to enable network and security monitoring, network planning, traffic analysis to include identification of network bottlenecks, IP accounting for billing purposes.

## Physical and Virtual Security Measures

**Anti-Malware:**

It's designed to detect, prevent, and remove malicious malware from computer systems. This includes viruses, worms, and trojan horses, and the purpose is to protect systems and data from unauthorized access and potential damage caused by malware.

**Intrusion Prevention Systems (IPS):**

IPS is a security technology designed to monitor and analyze network and/or system activities for malicious exploits or security policy violations. The purpose is to proactively identify and block known and unknown threats to maintain the security and integrity of the network.

**Intrusion Detection Systems (IDS):**

Similar to IPS, IDS monitors network and/or system activities to identify and alert to potential security incidents. However, IDS does not take preventive action; instead, it notifies administrators of suspicious activities. The purpose is to provide early detection of security threats, allowing for timely response and mitigation.

**Firewall:**

Acting as a barrier between a secure internal network and untrusted external networks, like the internet, it is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its goals are to prevent unauthorized access, monitor traffic, and establish a barrier against potential cyber threats.

**Encryption and Hashing:**

Encryption involves transforming data into a secure format, rendering it unreadable without the correct decryption key. It guarantees the privacy of classified data while being transmitted or stored. Hashing involves creating a fixed-size, unique hash value for data and providing data integrity verification.

**Surveillance Policy:**

Establishing clear standards for the morally and legally acceptable use of surveillance tools while guaranteeing the safety and security of the organization is the goal of a surveillance policy, which provides guidelines and rules regarding the use of surveillance technologies, such as cameras and monitoring systems. It also defines the scope of surveillance, acceptable use, and the handling of surveillance data.

**Doors (Access Control):**

Secure door access control is a type of physical security that controls who is allowed entry into buildings or certain areas within them. It works by using devices such as keycard access, PIN codes, or biometric scans to prevent unauthorized people from entering sensitive areas, safeguard property, and preserve the physical security of the property.

**Biometrics:**

Biometrics involves the use of unique physical or behavioral characteristics, such as fingerprints, retina scans, or facial recognition, for user authentication. Biometric systems enhance access control by ensuring that only authorized individuals gain entry. The purpose is to provide a highly secure method of identifying and verifying individuals based on their unique biological traits.

**Access Control Policy:**

The purpose of an access control policy is to establish regulations and guidelines for managing access to systems, networks, and physical locations. It clearly states the individuals who are granted access, the conditions for access, and the specific level of permissions they possess. The objective is to oversee and regulate user access to resources, guaranteeing the security and protection of sensitive data.

# **Appendix**

#### **Policies**

#### Revised Remote Access Policy for CyberBlast Crispy Company

1. **Overview**

Our team's productivity depends on having remote access to CyberBlast Crispy Company's corporate network. Nevertheless, we must take preventive action to reduce the hazards associated with potentially corrupted external networks.

2. **Purpose**

This policy attempts to reduce exposure to damages resulting from unauthorized use of company resources, losing confidential data, intellectual property, harm to the company's reputation, damage to vital internal systems, and financial liabilities. It does this by establishing guidelines and requirements for connecting to the CyberBlast Crispy Company's network from any host.

3. **Scope**

This policy covers remote access connections used for work-related activities, including email, intranet access, and any technical implementations of remote access to CyberBlast Crispy Company networks. All CyberBlast Crispy Company employees, contractors, vendors, and agents must adhere to this policy when using a company-owned or personal computer to access the network.

4. **Policy**

4.1 **General Usage**

The CyberBlast Crispy Company's network allows restricted recreational internet access to all its workers, vendors, contractors, and agents (authorized users).

Authorized users accessing the network from their personal devices must stop non-authorized users from accessing company resources. It is totally forbidden to engage in unlawful activity using the company network.

4.2 **Remote Access Requirements**

It must use encryption technologies, such as VPNs and strong passwords. For specific criteria, see the password policy and the VPN policy.

Even from relatives, authorized users need to protect their login credentials.

The remote host shouldn't be connected to any other network except personal networks under complete control while using the company-owned computer for remote access.

4.3 **Approval and Security Measures**

Using external resources to conduct CyberBlast Crispy Company business requires approval from InfoSec and the relevant business unit manager. All hosts connected to internal networks via remote access, including personal computers, must have the most recent version of anti-virus software installed. Third-party connections must adhere to the terms of the Third-Party Agreement. Any personal equipment used to access the network must meet the hardware and software configuration standards of CyberBlast Crispy Company.

5. **Policy Compliance**

5.1 **Compliance Measurement**

The InfoSec team will use a variety of techniques to evaluate compliance, such as feedback to the policy owner, internal and external audits, and reporting from business tools.

5.2 **Exceptions**

The InfoSec team will give approval for any exception to this policy.

5.3 **Non-Compliance**

Those employees who don't comply with the policy could face disciplinary measures, such as job termination.

6. Standards, policies, and processes that are interconnected.

* [Acceptable Encryption Policy](#_Revised_Acceptable_Encryption)
* [Password Policy](#_Revised_Password_Protection)
* [Server Security Policy](#_Revised_Server_Security)
* [Virtual Private Network (VPN) Policy](#_Revised_Virtual_Private)

#### Revised Virtual Private Network (VPN) Policy for CyberBlast Crispy Company

1. **Overview**

The VPN policy enhances CyberBlast Crispy Company's cybersecurity framework. This policy emphasizes the importance of VPNs for secure remote access. By using cutting-edge IT infrastructure, CyberBlast Crispy is streamlining operations and demonstrating its commitment to data security and technological innovation with the VPN policy.

2. **Purpose**

The CyberBlast Crispy Company network's remote access IPSec or L2TP virtal private network (VPN) connections are governed by the policies set forth in this policy.

3. **Scope**

This policy applies to all CyberBlast Crispy employees, contractors, consultants, and other employees, including third-party employees who use VPNs to access the CyberBlast Crispy network and to IT employees in specific. The policy specifically applies to VPN implementations directed through an IPSec concentrator.

4. **Policy**

1. VPNs are a "user-managed" service; approved CyberBlast Crispy Company employees and authorized third parties (customers, vendors, etc.) may use them; users choose the Internet Service Provider (ISP), arrange for installation, install any necessary software, and pay any associated fees. The Remote Access Policy contains more information.

1. Workers having VPN access rights are responsible to make sure that illegal users are blocked from accessing the internal networks of CyberBlast Crispy Company.
2. VPN use will be controlled using either onetime password authentication and a very strong password that contains 8 digits and a synonym.
3. VPNs compel all traffic to and from the PC over the VPN tunnel when it is actively connected to the business network; all other traffic is dropped.
4. Only one network connection is allowed, tunneling network is not permitted.
5. VPN gateways will be set up and managed by CyberBlast Crispy Company network operational groups.
6. The business norm is that all computers linked to the internal networks of CyberBlast Crispy Company, whether by VPN or another technology, must have the most recent version of anti-virus software.
7. Users of computers that are not CyberBlast Crispy Company-owned equipment must configure the equipment to comply with CyberBlast Crispy Company's VPN and Network policies.

5. **Policy Compliance**

5.1 **Compliance Measurement**

The team will verify compliance through various methods, including walk-throughs, business tool reports, internal and external audits, and feedback from the policy owner.

5.2 **Exceptions**

If there were exceptions to the policy, only the administrator should accept it.

5.3 **Non-Compliance**

An employee found to have violated this policy should be subject to disciplinary action, up to and including termination of employment.

#### Revised Server Security Policy for CyberBlast Crispy Company

1. **Overview**

Unsecured and vulnerable servers are significant entry points for malicious actors. Establishing consistent server installation policies, ownership, and configuration management is essential for robust cybersecurity practices.

2. **Purpose**

This policy aims to set standards for the base configuration of internal server equipment owned and/or operated by CyberBlast Crispy Company. Effective implementation will minimize unauthorized access to proprietary information and technology.

3. **Scope**

All employees, contractors, consultants, temporary workers, and others associated with CyberBlast Crispy Company must comply with this policy. It applies to server equipment owned, operated, or leased by the company or registered under its internal network domain. For secure configuration external to CyberBlast Crispy Company on the DMZ, refer to the Internet DMZ Equipment Policy.

4. **Policy**

4.1 **General Requirements**:

- Every internal server at CyberBlast Crispy Company must be owned by an operational group that oversees system administration.

- Based on business needs and with approval from the InfoSec team, each group must establish and maintain approved server configuration guides.

- Servers must be registered in the corporate enterprise management system, providing the necessary information for contact and identification.

- The management system must be kept up to date, and configuration changes for production servers must adhere to the proper change management protocols.

4.2 **Configuration Requirements**

- Operating system configuration should adhere to approved InfoSec team guidelines.

- Services and applications not in use must be disabled where practical.

- Access to services should be logged and/or protected through access control methods.

- Install the most recent security patches as soon as practical, with exceptions made only when immediate application interferes with business requirements.

- Avoid trust relationships between systems, using alternative communication methods when sufficient.

- Follow the principle of least required access, avoiding the use of root when a non-privileged account suffices.

- Perform privileged access over secure channels (e.g., encrypted network connections using SSH or IPSec).

- Physically locate servers in an access-controlled, secured environment, prohibiting operation from uncontrolled or unsecured cubicle areas.

4.3 **Monitoring**

- Report security-related events to InfoSec for evaluation and incident reporting.

- Log all security-related events on important or sensitive systems, keeping logs for predetermined periods of time.

5. **Policy Compliance**

5.1 Compliance Measurement the InfoSec team will use a variety of methods to confirm compliance, such as business tool reports, internal and external audits, and policy owner feedback.

5.2 Exceptions Any deviation from the policy requires prior approval from the InfoSec team.

5.3 Non-Compliance Violations may lead to disciplinary action, which may include termination of employment.

#### Revised Password Protection Policy for CyberBlast Crispy Company

1. Overview

At CyberBlast Crispy Company, passwords are the foundation of cybersecurity. We place a high value on the strength and confidentiality of our passwords because they are the first line of defense against unauthorized access and the possible exploitation of sensitive data. All employees, contractors, and vendors who have access to CyberBlast Crispy systems are responsible for following the guidelines below to ensure that their passwords are strong and secure.

2. Purpose

We hope to strengthen our cybersecurity posture and preserve our digital assets by offering clear guidelines on password creation, use, change, and protection. This policy serves to create a standard for the secure use and protection of all work-related passwords within CyberBlast Crispy Company.

3. Scope

This policy includes all personnel associated with CyberBlast Crispy Company, accessing the CyberBlast Crispy network, or handling non-public CyberBlast Crispy information.

4. Policy

4.1 Password Creation and Use

4.1.1 All user-level and system-level passwords must adhere to the Password Construction Guidelines.

4.1.2 Every account has its uniqueness. Work-related passwords should not be used for personal accounts.

4.1.3 Employees may handle and save work-related passwords securely by using approved password managers.

4.1.4 User accounts with system-level access must have a unique password, and the usage of multi-factor authentication is highly recommended for privileged accounts.

4.2 Password Change

4.2.1 Regular password expiration is not advised; passwords should only be updated in reaction to a suspected intrusion or failure to meet Password Creation Requirements.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are treated as sensitive, confidential CyberBlast Crispy information.

4.3.2 Passwords should not be inserted into email messages or disclosed over the phone.

4.3.3 Authorized password managers are the only permissible storage for passwords.

4.3.4 The "Remember Password" feature of applications should not be used.

4.3.5 Any individual suspecting a compromised password must report the incident and promptly change all relevant passwords.

4.4 Application Development

Application developers must incorporate the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Passwords should not be stored in clear text or any easily reversible form.

4.4.3 Passwords must not be transmitted in clear text over the network.

4.4.4 Applications should provide role management to enable one user to assume another's functions without knowing their password.

5. Policy Compliance

5.1 Compliance Measurement: The team will assess compliance through various methods, including business tool reports, internal and external audits, and feedback mechanisms for the policy owner.

5.2 Exceptions: Any exception to the policy requires prior approval from the team.

5.3 Non-Compliance: Violations may result in disciplinary action, up to and including termination of employment.

#### Revised Acceptable Encryption Policy for CyberBlast Crispy Company

1. Overview

See Purpose.

2. Purpose

This policy's main goal is to offer comprehensive guidelines that limit the use of encryption to algorithms that have been subjected to extensive public review and have been shown to be effective. It also seeks to guarantee adherence to federal regulations and legal authorization for the distribution and application of encryption technologies outside of the United States.

3. Scope

This policy applies universally to all employees and affiliates of CyberBlast Crispy Company.

4. Policy

4.1 Algorithm Requirements

4.1.1 Ciphers utilized must meet or surpass the criteria defined as "AES-compatible" or "partially AES-compatible" in the IETF/IRTF Cipher Catalog. Alternatively, they should align with the set specified in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2 or any superseding documents based on the date of implementation. Strongly recommended for symmetric encryption is the use of the Advanced Encryption Standard (AES).

4.1.2 Algorithms in use must comply with the standards outlined in NIST publication FIPS 140-2 or any superseding document based on the date of implementation. The use of RSA and Elliptic Curve Cryptography (ECC) algorithms is highly recommended for asymmetric encryption.

4.1.3 Signature Algorithms

|  |  |  |
| --- | --- | --- |
| Algorithm | Key Length (min ( | Additional Comment |
| ECDSA | P-256 | Consider RFC6090 to avoid patent infringement |
| RSA | 2048 | Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required. |
| LDWM | SHA256 | Refer to LDWM Hash-based Signatures Draft |

4.2 Hash Function Requirements

CyberBlast Crispy Company adheres to the NIST Policy on Hash Functions.

4.3 Key Agreement and Authentication

4.3.1 Elliptic curve Diffie-Hellman (ECDH), IKE, or Diffie-Hellman (Diffie-Hellman) must be used for key exchanges.

4.3.2 Endpoints need to be authenticated before session keys can be exchanged or derived.

4.3.3 Public keys that are used to establish trust need to be authenticated before they can be used. Examples of this include transmission via cryptographically signed messages or manual verification of the public key hash.

4.3.4 All servers used for authentication (like RADIUS or TACACS) must have a valid certificate signed by a known, trusted provider.

4.3.5 All servers and applications that use SSL or TLS must have certificates signed by a recognized, trusted provider.

4.4 Key Generation

4.4.1 Cryptographic keys must be generated and stored securely, preventing loss, theft, or compromise.

4.4.2 Key generation must be seeded from an industry-standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1 Compliance Measurement: The Infosec team will verify compliance through various methods, including business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions: Any exception to the policy must be approved by the Infosec team in advance.

* 1. Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# **REFERENCES**

* https://safetyculture.com/topics/risk-assessment/
* https://www.sans.org/information-security-policy/?page=2
* https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0759f19972ec623e/5e9dd1fa33f6b8718946a2b9/acceptable\_encryption\_policy.pdf
* <https://siteglobal.com/system/files/2021-10/Sample%20Safety%20and%20Security%20Policy.pdf>
* **How IT security can be aligned with an organizational policy, detailing the security impact of any misalignment**

An organization's components may not be in agreement with each other in cybersecurity efforts; this is known as security misalignment. It can happen at different level's, such as between the Chief Information Security Officer and other executives, between CISOs and the Chief Information Officers CIOs, or even between organizational policies and IT security policies.

Aligning security objectives with more general business goals becomes so difficult if the CISO is not included in discussions with the other executives, which happen's to be the case in many businesses where the CISO may not have an equal voice in strategic decision-making processes and It is possible to develop misunderstandings, conflicting priorites, and a lack of a shared vision for cybersecurity risk's if there are no communication channels between the security team and other departments.

The CISO and CIO may have different priorities and objectives. While the CISO is primarily concerned with securing the organization's information assets, the CIO is focused on the efficent functioning of IT systems to support business operations. Without a shared understanding and collaboration, these priorites can clash and lead to misalignment, there will also be security misalignment's when there is a disconnect between the enterprises tolerance for risk and the security functions risk management approach. Failure to establish a common understanding of acceptable risk levels can lead to inadequacies in security measures or unnecessary constraints on business operations.

The organization's may have policies that govern different aspects of their operations. When there is a misalignment between these general policies and specific IT security policies, it will lead to non-compliance, security gap's, increased vulnerability to cyber threats, and leave security vulnerabilities unaddressed, making the organization more suscepteble to cyberattacks.

If chiefs and the board don't agree with each other regarding acceptable levels of risk, the security team may struggle to implement measures that appropriately extenuate threat's without impeding business operations.

**Remote Access Policy Misalignment:**

Lack of commitment to adhere to the Cyberblast Crispy Company's Remote Access Policy could cause an unauthorized or insecure remote access, posing risks such as data breaches, compromise of sensitive information, and potential harm to the companys reputation. Ensure that all remote access connections strictly follow the Remote Access Policy guidelines, incorporating encryption technologies, robust password's, and compliance with approval and security measures, the organization's policy owners work closely with the IT security team, regularly review and update the policy to address emirging threats and maintain a secure remote access environment.

**VPN Policy Misalignment:**

Misalignment with the Cyberblast Crispy Companys VPN Policy may result in weak VPN configurations, leading to unauthorized access, data interception. Align VPN configurations with the VPN Policy, emphasizing user responsibility for securely managing VPN services. Regularly update VPN gateways, enforce strong authentication measures, and monitor compliance to prevent security vulnerabilites and maintain a resilient VPN infrastructure, and make sure the employees are following the policies for the VPN.

**Server Security Policy Misalignment:**

Lack of commitment to the Cyberblast Crispy Company's Server Security Policy may expose vulnerabilities in server configurations, leading to unauthorized access or data breaches. So, we have to make sure that servers strictly adhere to the Server Security Policy by implementing approved configurations, promptly applying security patches, and following proper change management procedures. Regularly monitor and log security-related events to detect and respond to potential threat's and maintaining the integrity of server security.

**Password Protection Policy Misalignment:**

Non-compliance with the Cyberblast Crispy Company's Password Protection Policy could result in weak passwords like using short and guessable words for the password, or not combining between the letters and numbers and symbols this will lead to guess the password faster and to unauthorized access, identity theft, or compromise of sensitive information. Apply the Password Protection Policy by promoting strong password creation, secure handling, and update frequently to make sure that consistency and adherence to security best practices. Educate users on password security and consider implementing multi-factor authintication for privileged accounts to enhance overall password security, and make sure that the organizations policy owner's work closely with the IT security team.

**Acceptable Encryption Policy Misalignment:**

Going far from the Cyberblast Crispy Company's Acceptable Encryption Policy may cause an insecure communication, data breaches, or legal and regulatory repercussions. So, we have to make sure that encryption practices align with the Acceptable Encryption Policy, including the use of approved algorithms, proper key management, and adherence to industry standard's and assess and consistently upgrade encryption technologes to proactively address ever-changing security risks and maintain compliance with the companys encryption standards.

CyberBlast Crispy can enhance its security posture and mitigate the risk of security incidents by the effective cooperation and communication between policy owners and the IT security teams, also they should create communication channels to facilitate the exchange of insights, updates on emerging threats, and policy adjustments. This cooperation allows for a more holistic understanding of security requirement's, which will enable policymakers to craft guidelines that are compliant. All this will help CyberBlast Crispy to proactively address vulnerabilities, implement robust security control's, and maintain a resilient security posture across its operations.