CYB60004 – Network and Cybersecurity Framework

Assignment 2

Security plan

Pulkit Patel

103139787

Executive Summary

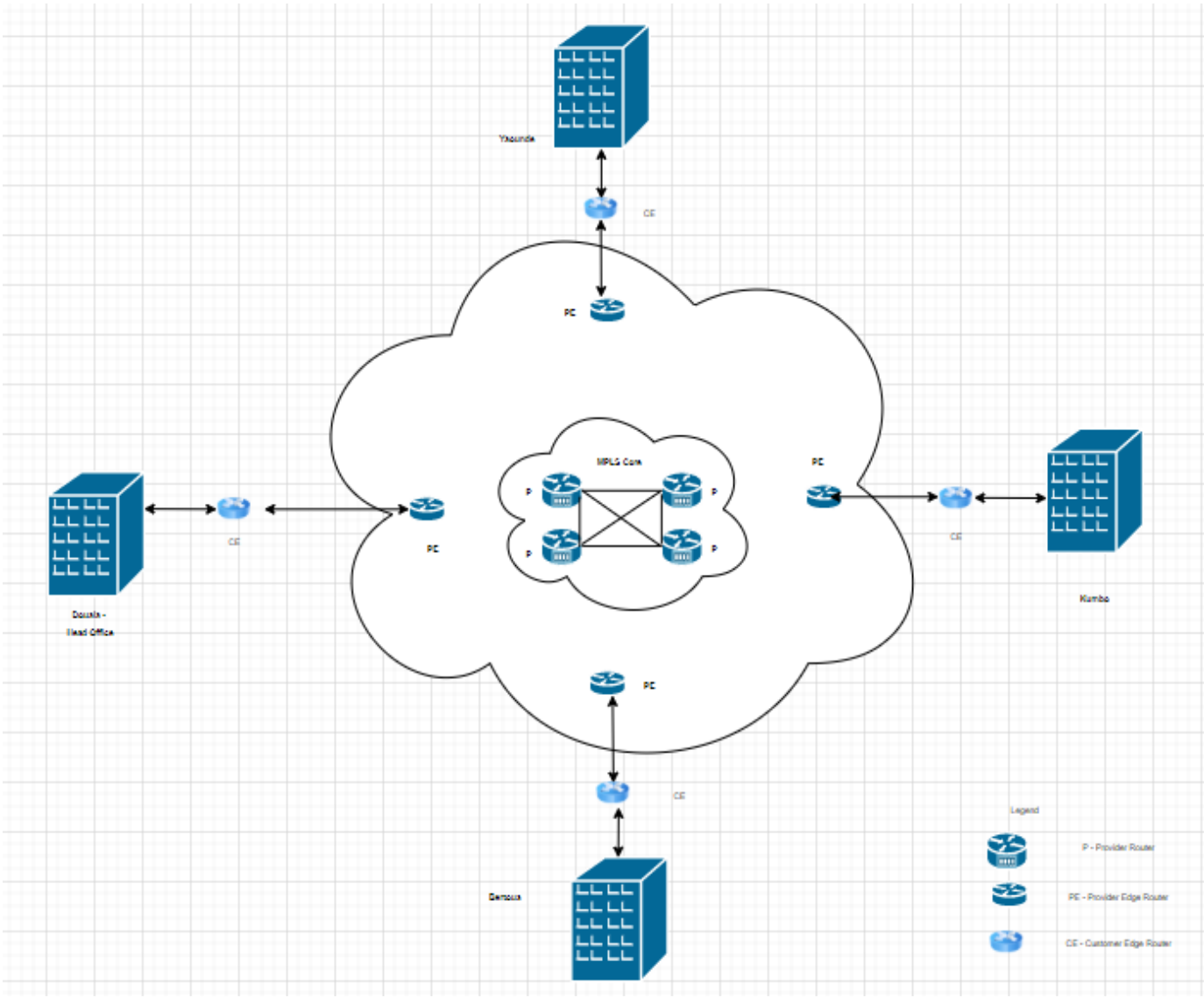
This task examines my awareness of network security. I encourage our organization to take a holistic approach to understanding our architecture and inventory in places. This task is divided into different parts. The web project proposal is the first part. Risk analysis is another part. Physical security is the third part. The IT security audit section is the fourth section. Infrastructure security is the fifth part. Security of human resources is the last and sixth part.

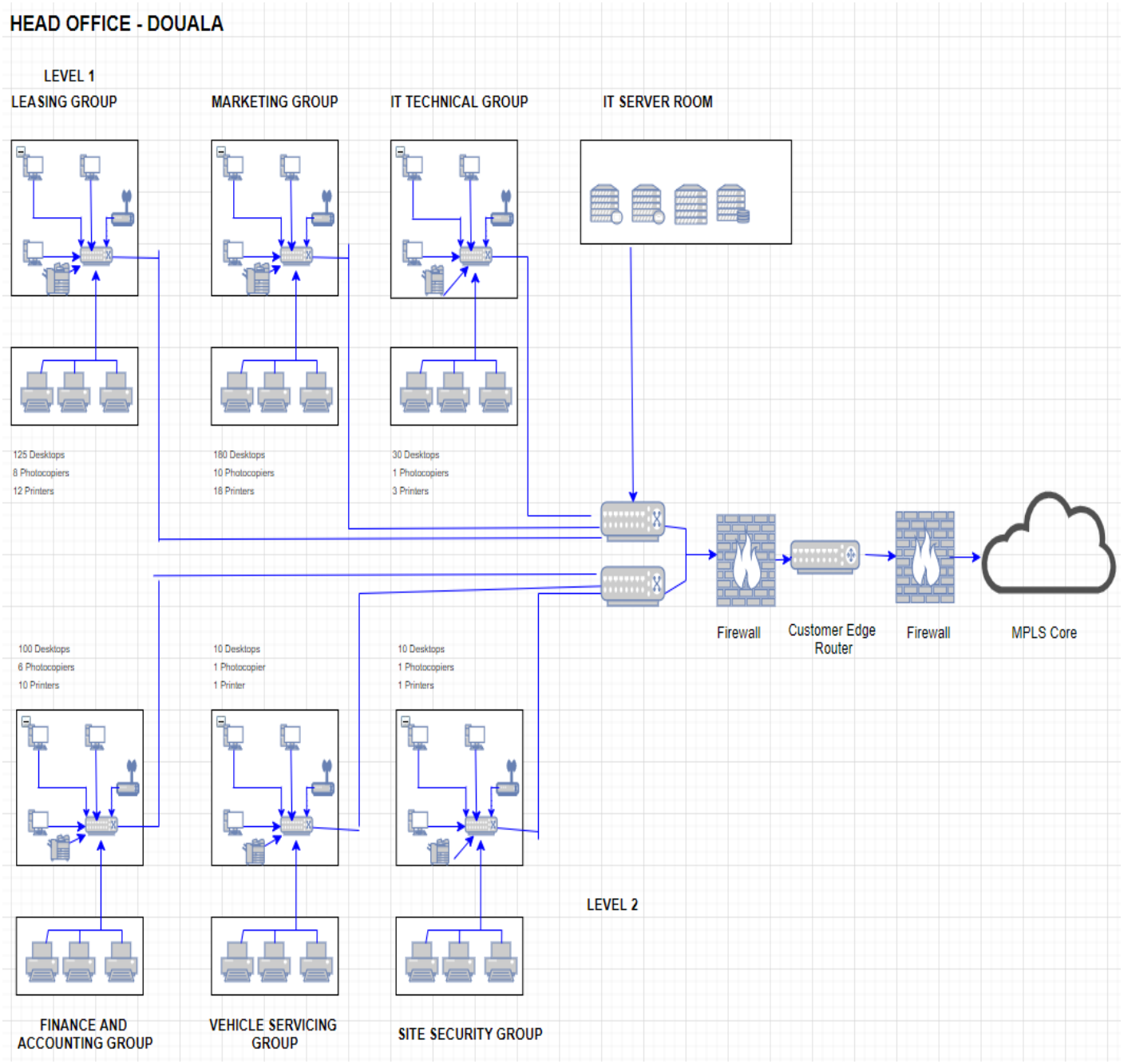
Table of Contents

Introduction

Our organization depends on data confidentiality, integrity, and availability. Our data cannot be created without the means used to collect the data. It includes human resources, structures or buildings, hardware, software, and procedures. We often overlook the importance of planning to protect our investments. Assets can be destroyed in an instant and become a source of danger from time to time, causing serious damage to the company. Therefore, we must prepare to secure the assets and resources of our company. To secure your assets and resources, a top-down approach is used when creating a security plan. I researched the criteria to get an in-depth look at structure, size, location, and purpose. The information obtained from the risk analysis together with the network planning identifies the risks and weaknesses and the success criteria. That's why I offer our company's network security plan, IT protection management and human security management. Personnel security is necessary to protect the digital assets of the organization and customers, such as information and IT infrastructure ("Network Security Planning", 2018). As a result, total security is required. All servers handling our company's critical data must be in a secure area with appropriate physical security measures such as locks and security personnel and must be cordoned off.

Network Diagram




HEAD OFFICE - DOUALA
LEVEL 1
LEASING GROUP
MARKETING GROUP
IT TECHNICAL GROUP
IT SERVER ROOM
125 Desktops
8 Photocopiers
12 Printers
180 Desktops
10 Photocopiers
18 Printers
30 Desktops
1 Photocopiers
3 Printers
Firewall
Customer Edge Router
Firewall
MPLS Core
100 Desktops
6 Photocopiers
10 Printers
10 Desktops
1 Photocopier
1 Printer
10 Desktops
1 Photocopiers
1 Printers
LEVEL 2
FINANCE AND ACCOUNTING GROUP
VEHICLE SERVICING GROUP
SITE SECURITY GROUP

Risk analysis

The assets of Ground Clearance Oy are divided into two categories: physical assets and information assets. We have documented all the network and security devices we use in our physical assets. Examples of data resources are files, forms, websites, customer information and any computer information.

Physical Assets:-

Douala, headquarters

455 desktops/laptops, 45 printers, 27 copiers, 2 routers, 2 firewalls, 8 switches and 4 servers.

Yaounde site

92 desktops/laptops, 10 printers, 6 copiers, 2 routers, 2 firewalls, 8 switches and 4 servers.

Kumbo site

154 desktops/laptops, 15 printers, 10 copiers, 2 routers, 2 firewalls, 8 switches and 4 servers.

Bertoua's site

135 desktops/laptops, 14 printers, 9 copiers, 2 routers, 2 firewalls, 8 switches and 4 servers.

Identify Potential Hazards:-

Server failure, flood to damage infrastructure, fire, sabotage, extortion, unauthorized system access, hacking, fraud, communication failure, hardware failure, unauthorized access or use, Pc's stolen, human error, power lost.

Identification of Risks and Likelihood Impact Analysis:-

The current threats and threats of each hazard are listed in the two tables below. It describes risk of Company's network. we find risk and impact of company.

Risk No	Vulnerability	Threat	Risk of Compromise of	Risk Summary
1	Wet-pipe sprinkler system in Data Center.	Fire	Availability of and data	Fire would activate sprinkler system causing water damage & compro-mising the availability of the site
2	User identifiers (IDs) no longer required are not removed from in timely manner.	Unauthorised Use	Confidentiality & integrity of data	Unauthorised use of unneeded user IDs could compromise confidentiality & integrity of data.
3	Access privileges are granted on an ad-hoc basis rather than using predefined roles.	Unauthorised Access	Confidentiality & integrity of data	Unauthorised access via ad-hoc privileges could compromise of confidentiality & integrity of data.
4	New patches to correct flaws in application security design have not been applied.	Malicious Use Computer Crime	Confidentiality & integrity of data	Exploitation of un-patched application security flaws could compromise confidentiality & integrity of data.
5	User names & passwords are in scripts & initialisation files.	Malicious Use Computer Crime	Confidentiality & integrity of data	Exploitation of passwords in script & initialisation files could result in compromise of confidentiality & integrity of data.
6	Passwords are not set to expire; regular password changes are not enforced.	Malicious Use Computer Crime	Confidentiality & integrity of data	Compromise of unexpired/unchanged passwords could result in compromise of confidentiality & integrity of data.
7	"Generic" accounts found in the database (e.g., test, share, guest).	Malicious Use Computer Crime	Confidentiality & integrity of data	Use of generic accounts could result in compromise of confidentiality & integrity of sensitive data.
8	Remote OS authentication is enabled but not used.	Malicious Use Computer Crime	Confidentiality & integrity of data	Remote access is not currently used by ; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive data.
9	Login encryption setting is not properly configured.	Malicious Use Computer Crime	Confidentiality & integrity of data	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive data.
10	Sensitive data is not backed up	Malicious Use Computer Crime	Integrity and Availability of data.	Loss of data could compromise integrity, availability of data.
11	Ransomware virus infects database and locks up servers	Unauthorised access to system Network Intrusion Computer Crime	Confidentiality Availability and Integrity	Protection on system is not up to date and employee training is not being managed so virus gets through and locks up system database and servers.
12	Un-updated software is not secured by new patches.	Malicious use Human error	Software errors affecting Availability and Integrity of data	Technicians are not updating firmware and software regularly which leave possible vulnerabilities in security hardware
13	Power Failure causes loss of data and corruption in data	Human Error Power Loss	Availability and integrity of data	Over the last 12 months, the local coal-fired power station has been decommissioned—the site is now subject to intermittent power failures. Any event that causes power outage that causes us to lose power and data is lost or corrupted.
14	Monitoring of the network is not sufficient	Human Error Network Intrusion	Confidentiality and Integrity of data and network transmission	Over the last 12 months, use of photocopiers has been excessive. The current security used to monitor the device is not properly configured and our packets, and data could be monitored by Unauthorised users.
15	Head office prone to flooding	Flood	Availability and integrity of data.	There was a breaking over the last month and number of PCs were stolen
16	Break-in at the Bertoua and other sites	Physical Intrusion	Availability and integrity of data.	Over the last 12 months, the city council has redirected a river to create a park—the site is now prone to flooding.

Risk No	Risk2	Likelihood	Impact	Total Risk Score
1	Wet-pipe sprinkler system in Data Center	6	6	36
2	User identifiers (IDs) no longer required are not removed from in timely manner	3	4	12
3	Access privileges are granted on an ad-hoc basis rather than using predefined roles	2	5	10
4	New patches to correct flaws in application security design have not been applied	3	1	3
5	Usernames & passwords are in scripts & initialization files	4	3	12
6	Passwords are not set to expire; regular password changes are not enforced	2	4	8
7	"Generic" accounts found in the database (e.g., test, share, guest)	2	6	12
8	Remote OS authentication is enabled but not used	3	3	9
9	Login encryption setting is not properly configured	6	6	36
10	Sensitive data is not backed up	4	6	24
11	Ransomware virus infects database and locks up servers	5	4	20
12	Un-updated software is not secured by new patches	2	2	4
13	Power Failure causes loss of data and corruption in data	3	1	3
14	Monitoring of the network is not sufficient	6	3	18
15	Head office prone to flooding	6	6	36
16	Break-ins at the Bertoua and other sites	6	6	36

As the above table illustrates, the largest risks are numbers 1, 9, 15, and 16.

1 is damage network infrastructure it happens by an accidently.

9 is shows the right policy is not properly set so set properly. This help to access Unauthorized users to view the files. This risk implements by set proper policies in the network system. Give the right permission to user account.

Head office prone to flooding because of the new direction of river to construct the park. This is very risk for head office. We need to talk with city council for this situation. It affects to company's employees.

The risk at Bertoua site is stolen pcs because of security guards. We suggest adding 2 security guard in this site.

Physical Security

Access systems:

Install access control systems such as key cards, biometric scanners or PIN codes at building entry points and critical locations, including IT server rooms. Limit access to authorized personnel only and implement the principle of least privilege.

CCTV surveillance:

Strategically use CCTV cameras to monitor and record activity in premises including entrances, server rooms and warehouses. Ensure that the CCTV system is in good working order and that the recordings are securely stored.

Physical barrier protection:

Install physical barriers such as fences and gates to control access to the property and prevent unauthorized entry. Make sure the fence is in good condition and that it is inspected regularly.

Environmental control:

Use environmental monitoring sensors to detect and alert workers to potential hazards such as temperature fluctuations, humidity and flooding in IT server rooms and other critical areas. Integrate environmental monitoring system with network monitoring system for active operation.

Guardians:

Use trained security guards to patrol the site and physical presence as a deterrent. Security guards should be located at main entry points and regularly patrol the buildings. Manage

visitors:

Implement a visitor management system to record and track visitors entering the site. Issue temporary access cards or visitor cards that restrict access to certain areas.

Secure Storage:

Use secure cabinets and safes to store sensitive documents, keys, or backups. Restrict access to these storage areas to authorized personnel only.

Remote monitoring:

If possible, set up remote monitoring capabilities so that security or IT personnel can access monitoring streams and environmental data off-site.

Lighting:

Provide adequate exterior lighting around the site, especially in parking lots and entrances, to improve visibility and prevent unauthorized activity after dark.

Security awareness and training:

Train employees on physical security best practices, including the importance of securing workplaces, locking doors, and reporting suspicious activity. Conduct drills to practice emergency operations, including evacuation.

Alarm systems:

Install an intrusion detection system in critical areas such as server rooms and warehouses. Connect alarm devices to monitoring centre or security personnel to immediately respond to unauthorized access attempts.

Removal of sensitive material:

Implement secure shredding and disposal procedures for sensitive documents and media such as hard drives and backup tapes. By implementing these physical security measures, Ground Clearance Oy can significantly improve the protection of its physical assets, IT infrastructure and sensitive data in all its locations. It is important to regularly review and update physical security policies to combat new threats and maintain a secure environment.

IT Security Control

Firewalls:

Install and configure firewalls at each location to monitor and control incoming and outgoing network traffic. Implement access control lists (ACLs) to restrict unauthorized access to critical services and ports. Install firewalls with intrusion prevention capabilities to detect and block malicious activity. Intrusion Detection and

Prevention Systems (IDPS):

Use IDPS anywhere to monitor network traffic for suspicious or unauthorized activity. Configure IDPS to trigger an alarm or block traffic in real time when potential threats are detected.

Data encryption:

Encrypt sensitive data, especially when transmitted over the network, using protocols such as SSL/TLS for network traffic and VPN for remote access. To protect data at rest, enable encryption on storage devices and backups.

Strong authentication:

Use strong passwords and implement a password policy that requires regular passwords. Enable multi-factor authentication (MFA) for critical systems and remote access to improve user authentication.

Access Control and Least Privilege:

Implement role-based access control (RBAC) to grant users the minimum privileges necessary to perform their job duties. Limit administrator access to critical systems and limit the number of privileged accounts.

Network segmentation:

Segment the network into separate VLANs to isolate sensitive data and limit lateral movement of potential attackers.

Registration and Tracking:

Configure centralized logging and network activity to identify and investigate suspicious events. Maintain logs for an appropriate period to ensure incident investigation and compliance. Physical

security:

Implement physical security measures such as access control systems and CCTV monitoring to protect IT server rooms and critical infrastructure. Monitor environmental factors such as temperature and humidity to prevent damage to the device. Backup and

disaster recovery:

Back up important data and systems regularly by keeping backups in secure locations. Develop a comprehensive disaster recovery plan to ensure business continuity in the event of a cyber or natural disaster.

Event schedule:

Develop and document a contingency plan that outlines the actions to be taken in the event of a security breach or cyber-attack. Conduct periodic exercises and drills to test the effectiveness of incident response procedures. By implementing these IT security controls, Ground Clearance Oy can significantly improve its network security position and reduce the risk of cyber-attacks and potential data breaches at all of its locations.

Network Security Devices	Risk Number Mitigated
F HFC-227ea and FM-200 Fire Suppression System	1
Firepower 4150 NGIPS	2 3 5 6
ASA 5555-X with Firepower Services	9
Cisco Security Packet Analyzer 2400	10 14
Oracle MDM System Servers	10
Cisco Secure Network Server 3595	2 3 5 6 8 9 11 12
Cisco Intrusion Detection System 4215 SENSOR	11 14
Cisco ASR 1001 VPN and Firewall Bundle Router	2 3 5 6 9
APC Smart-UPS RT AC 220/230/240 V 16 kW 20000VA	13
Gemini™ MPS Twin Pack 5000 kW	13

Software to Assist with Risk Mitigation:-

We use various applications to increase network control. We follow the rules and standards necessary to reduce the risks listed above. To do this, we use network software and CISCO services to monitor network threats and prevent malicious attacks. The new security software to be installed is listed in the table below, as is the device above.

Network Security Applications	Risk Number Mitigated
Cisco Adaptive Security Device Manager	11 13
Cisco Stealth Watch Monitoring Service	10 13
Cisco Prime Network	2 3 4 5 7 10 13
Oracle MDM Applications	9
Identity Services Engine Access Control System	3 4 5

Infrastructure Security

Secure network architecture:

Design and implement a secure network architecture where sensitive data and services are properly segmented and isolated. Use VLANs and Access Control Lists (ACLs) to control traffic flow and restrict access to specific resources.

Network firewalls:

Deploy network firewalls at each location to monitor and manage inbound and outbound traffic. Configure firewalls to monitor security policies and prevent unauthorized access attempts.

Intrusion Detection and Prevention Systems (IDPS):

Enable IDPS to monitor network traffic and detect potential security breaches or suspicious activity. Configure IDPS to automatically respond or notify administrators of detected threats.

Secure wireless network:

Protect your wireless network with strong encryption (WPA2 or WPA3) and strong authentication methods such as WPA2-Enterprise 802.1X. Update your wireless access point's firmware regularly to fix vulnerabilities.

Continuous monitoring:

Implement continuous monitoring solutions to track network activity, device health and performance metrics. Use log management and security information and event management (SIEM) tools to identify and investigate security incidents.

Backup and Restore:

Back up important data and settings regularly by keeping backups safely and elsewhere. Test data recovery regularly to ensure data integrity and reliable disaster recovery.

Vendor Management:

Comply with security requirements and perform security assessments of third-party providers of critical infrastructure components. Monitor and ensure vendor compliance with security standards. By implementing these infrastructure security measures, Ground Clearance Oy can strengthen the protection of its IT assets, protect itself against cyber threats, and improve the overall resilience of the network at all locations. Continuous monitoring and updating of security measures are necessary to adapt to changing threats and maintain a secure IT environment.

Human Resources Security

Employee Background Check:

Complete a thorough background check, including criminal and employment history, prior to employment. Ensure that employees who have access to sensitive information undergo more thorough vetting.

Security awareness training:

Conduct regular security training for all employees to educate them on cybersecurity risks, best practices, and company security practices. Train employees to identify and report potential security breaches.

Acceptable Use Policy (AUP):

Create and enforce an acceptable use policy that defines acceptable practices for the use of company IT resources and Internet access. Communicate the AUP to all employees and obtain their approval.

Procedure for terminating an employee:

Establish procedures to immediately revoke access to IT systems and physical facilities when an employee resigns or leaves the company. Conduct exit interviews so that employees understand their responsibilities for protecting companies after they leave the organization.

Awareness of social manipulation:

Train employees on social engineering techniques such as phishing so they can recognize potential pitfalls and avoid them. Run simulated phishing campaigns to assess and improve employee awareness.

Remote work security:

Implement security measures for remote workers, such as secure VPN connections, multi-factor authentication, and secure file transfer protocols. Ensure remote workers follow the same safety policies and procedures as on-site workers.

Third-Party Protection:

Ensure that third-party vendors and contractors who have access to the company's network or sensitive information adhere to the company's security requirements. Regularly review and evaluate the security of third-party service providers.

Safe workplace practices:

Encourage employees to lock their workstations when away from their desks to prevent unauthorized access. Enable automatic workstation locks after a certain period of inactivity. By implementing these human resource security measures, Ground Clearance Oy can promote a security-aware culture and reduce the risk of insider threats. Regular training and clear policies help ensure that employees understand their responsibilities for maintaining network security and protecting sensitive information.

Conclusion:-

In summary, it can be stated that the implementation of a comprehensive network security plan with strong monitoring of IT security, physical security measures, infrastructure security and human resource security will significantly improve the network security position of Ground Clearance Oy and protect its valuable and sensitive assets. information in all facilities. websites

By appointing an IT security manager and conducting a thorough risk analysis, a company can identify potential threats and vulnerabilities, allowing them to prioritize and effectively allocate resources to mitigate risks. Implementation of firewalls, intrusion detection and prevention systems, and data encryption will strengthen the network against cyber threats and unauthorized use.

The plan's focus on physical security, such as access systems, CCTV surveillance and environmental monitoring, protects the company's IT infrastructure and server rooms against physical intrusions and environmental risks. In addition, incorporating personal security measures (including employee background checks, security awareness training and data access management) promotes a security-aware culture and reduces the risk of insider threats. In addition, regular monitoring, patch management, and incident response planning ensure a proactive approach to network security and enable a quick and efficient response to information security incidents or breaches. Third-party security assessments ensure that all parties with access to the company's network meet the required security standards.

Overall, the network security plan strengthens Ground Clearance Oy's defences against cyber-attacks and data breaches, strengthening its commitment to protecting operations, data, and reputation. By continuously improving and adapting to new threats, the company is better able to maintain business continuity and protect its customers, employees, and stakeholders in an increasingly digital and interconnected world.

References:-

Den Boer, M. (2015). Juggling the Balance between Preventive Security and Human Rights in Europe. *Security and Human Rights*, 26(2-4), pp.126–146. doi:https://doi.org/10.1163/18750230-02602009.

Leverrier, A. and Grangier, P. (2010). Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation. *Physical Review A*, 81(6). doi:https://doi.org/10.1103/physreva.81.062314.

'Secure VPN Design Considerations' 2003, *Network Security*, vol. 2003, no. 5, pp. 5–10.

Secure domain unit for network protection. (1996). *Network Security*, 1996(1), pp.5–6. doi:https://doi.org/10.1016/s1353-4858(96)90162-2.

Wang, W. and Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, [online] 57(5), pp.1344–1371. doi:https://doi.org/10.1016/j.comnet.2012.12.017.