# RISK ASSESSMENT REPORT

**System/Asset:** ***HASO OPTICAL AND EYE CARE FACILITY***

**Date: 25 November, 2024**

**Risk assessment Team**

| Name | Designation |
|---|---|
| Jude Assafuah Rodrigo | **IT manager** |
| Patience Sturridge Taglifico | **Senior IT officer** |
| Ernest Dadson Kukurantumi | **Senior Compliance officer** |
| Samuel Melchizedek Osei | **Risk assessment and compliance officer** |

### Executive summary

This risk assessment identifies and evaluate the potential threats and risks to HASO OPTICAL AND EYE CARE FACILITY's virtual private network server (Nord VPN) and Microsoft Exchange. Virtual private network (VPN) is a connection over the internet where the system is system is secured and encrypted between the end users. VPN ensures the IP address and location are masked or protected when accessing the organization system remotely. Microsoft Exchange is a messaging platform that provide email, calendar, contact and tasks. It runs on windows operating system. VPN and Microsoft Exchange are critical component of the IT infrastructure of the facility and therefore must properly configured and managed to ensure smooth operation of the facility. The assessment highlights significant vulnerabilities and provides recommendations to mitigate identified risks

### Assessment objective

The objective of this assessment is to formulate a comprehensive assessment report which includes risk assessment portfolio, risk register, detailed mitigation strategies for the identified threats and risk matrix.

### Scope

The scope of the risk assessment is to identify and evaluate potential risks to the virtual private network (Nord VPN) and Microsoft Exchange servers used by the facility. It details the vulnerabilities, likelihood, impact and mitigation strategies of this risk on the IT infrastructure especially the Microsoft exchange and VPN server.

## System assessed: Nord Virtual Private Network Server (Nord VPN)

| Threat identification | Malicious VPN deployment |
|---|---|
| vulnerabilities | • IP address exposure<br>• Weak encryption algorithm<br>• Poor server security<br>• DNS leaks |
| Likelihood | 3 |
| Impact | 4 |
| Mitigation strategies | • Antivirus deployment<br>• Strong password policy<br>• Multifactor authentication<br>• Awareness and training |

| Threat identification | Man-in-the middle |
|---|---|
| vulnerabilities | • Vulnerable VPN software<br>• Weak SSL/TLS configuration<br>• Unsecured Wi-Fi network<br>• Unvalidated HTTPS certificate |
| likelihood | 2 |
| Impact | 4 |
| Mitigation strategies | • Implement IDS/IPS<br>• Implement HTTPS validation certificate<br>• Implement secured SSL/TLS configuration |

| Theat identifcation | Distributed Denial of service (DDOS) |
|---|---|
| vulnerabilities | • Insecure network system<br>• Insufficient traffic filtering<br>• Insecure IoT devices |
| Likelihood | 2 |
| impact | 3 |
| Mitigation strategies | • Implement DDOS protection services<br>• Conduct regular system audit<br>• Implement incident response plan |

| Threat identification | Credential theft |
|---|---|
| vulnerabilities | • Unpatched software<br>• Weak password policy<br>• Poor server configuration<br>• Phishing attacks |
| likelihood | 4 |
| Impact | 2 |
| Mitigation strategies | • Multifactor authentication<br>• Incident response plan<br>• Awareness training |

| Threat identification | Malware and ransomware |
|---|---|
| vulnerabilities | - Poor server configuration<br>- Unvalidated user input<br>- Unsecured SSL/TLS connection<br>- Weak password and authentication |
| Likelihood | 3 |
| Impact | 5 |
| Mitigation strategies | - Strong password policy<br>- Multifactor authentication<br>- Awareness training<br>- Incident response plan |

| Threat identification | IP address and DNS leakage |
|---|---|
| vulnerabilities | - Poor server configuration<br>- Weak VPN protocols<br>- Unpatched software |
| Likelihood | 3 |
| Impact | 2 |
| Mitigation strategies | - Secured server configuration<br>- Strong VPN protocols<br>- Regular update of software |

## System assessed: Microsoft Exchange server

| Threat identification | Server hijacking |
|---|---|
| vulnerabilities | - Weak password policy<br>- Firewall misconfiguration<br>- Ineffective access control<br>- SQL injection |
| Likelihood | 2 |
| Impact | 5 |
| Mitigation strategies | - Multifactor authentication<br>- Effective access control<br>- Proper firewall configuration<br>- Incident response plan |

| Threat identification | Intercepted corporate emails |
|---|---|
| Vulnerabilities | - Phishing attacks<br>- Malware infected emails<br>- Ineffective email security gateway<br>- Spoofing and impersonation |
| likelihood | 3 |
| Impact | 4 |
| Mitigation strategies | - Multifactor authentication |

| | |
|---|---|
| | • Firewall configuration<br>• Antivirus and antimalware<br>• Awareness training |

| Threat identification | Data theft |
|---|---|
| vulnerabilities | • Weak password policy<br>• Unencrypted database<br>• Insider threat<br>• Privilege abuse<br>• Phishing attack |
| Likelihood | 4 |
| Impact | 4 |
| Mitigation strategies | • Strong password policy<br>• Strong encryption algorithms (AES-256)<br>• Deactivation of email account of terminated employee<br>• Awareness training |
| | |

| Threat identification | Man-in-the middle |
|---|---|
| vulnerabilities | • Unsecured network system<br>• Unpatched software<br>• Lack of IPS/IDS<br>• Weak encryption algorithms<br>• Misconfigured firewalls<br>• Weak SSL/TLS |
| Likelihood | 2 |
| Impact | 4 |
| Mitigation strategies | • Secured network connection<br>• Implementation of IPS/IDS<br>• Secured SSL/TLS<br>• Strong encryption algorithm<br>• Firewall installation |

| Threat identification | Insider threat |
|---|---|
| vulnerabilities | • Disgruntled employee<br>• Negligence of employee<br>• Weak access control<br>• Privilege abuse |
| Likelihood | 5 |
| impact | 4 |
| Mitigation strategies | • Strong access control<br>• Awareness training<br>• Implement Least privilege and Need-to-know<br>• Effective background check before employment |

| Threat identification | Malware and ransomware |
|---|---|
| vulnerabilities | • Weak IP address<br>• Weak password policy<br>• Weak server security<br>• Disgruntled employee<br>• Unsecured firewall configuration |
| Likelihood | 3 |
| Impact | 5 |
| Mitigation strategies | • Antivirus and antimalware<br>• Secured Firewall configuration<br>• Multifactor authentication<br>• Awareness training<br>• Strong server security |

## Conclusion

The risk assessment done on Nord VPN and Microsoft Exchange identified numerous critical risks that could impact the IT security and operation of HASO optical and eye care facility. By implementing this mitigation strategies and recommendations, the facility can reduce the likelihood and impact of the aforementioned threats to ensure security compliance, business continuity while achieving RTO and RPO.

## Control activities and recommendation

- Regular patching and updating software.
- Implementation of strong endpoint security.
- Implementation of physical security such guards and CCTV cameras.
- Enforcement of strong password policy and multifactor authentication.
- Regular user education on phishing and various awareness training.
- Effective background check on potential employees and contractors.
- Effective implementation of segregation of duties and compulsory leave for employees in the organization.
- Implementation of offsite and cloud backup of data.
- Implement Strong encryption algorithms (AES-256) on data in transit, at rest etc.
- Proper configuration of firewalls, antimalware and antivirus.
- Implement strong access control for all employees and senior staff.
- Service level agreement with third party service providers to ensure RTO.
- Regular maintenance and monitoring of servers.

| Level | likelihood | Impact |
|---|---|---|
| 1 | Rare | Acceptable level |
| 2 | unlikely | Bad |
| 3 | likely | Serious |
| 4 | Very likely | Severe |
| 5 | Frequent | Catastrophic |

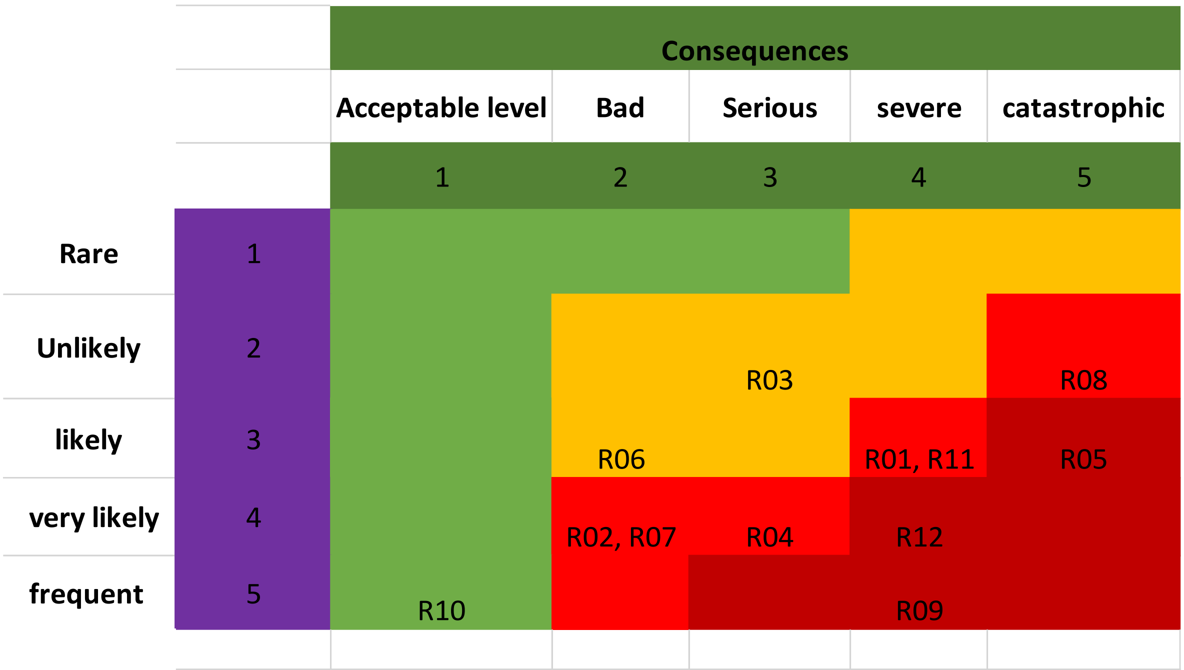
# IT RISK REGISTER

Surpervisor: Ben Bovin PhD

HASO OPTICAL FACILITY
RISK REGISTER 2024-RR02
LAST REVIEW: 27 NOV 2024
NEXT REVIEW: 20 NOV 2025

| RISK I | RISK DESCRIPTION | LIKELIH | IMPACT | EXISTING CONTROL | MITIGATION | RISK LEVEL | RISK OWNER |
|---|---|---|---|---|---|---|---|
| R01 | Malicious VPPN | 3 | 4 | Incident response plan | 1. strong VPN configuration<br>2.strong pasword policy and MFA | HIGH | IT securityofficer |
| R02 | Man-in-the-middle | 2 | 4 | access control policy | 1. implement IDS/IPS<br>2. Secure SSL/TLS protocols | HIGH | IT securityofficer |
| R03 | DDOS | 2 | 3 | Incident response plan | 1. Implement DDOS protection serve<br>2. regular system audit | MEDIUM | Network administrator |
| R04 | credential theft | 4 | 3 | access control policy | 1. regular loggin audit<br>2. strong password policy and MFA | HIGH | Access control manager |
| R05 | Malware/ransonware | 3 | 5 | Incident response plan | 1. sttrong password and MFA<br>2. AWARENESS training | EXTREME | Network administrator |
| R06 | IP address&DNS Leak | 3 | 2 | Data privacy policy | 1. secured VPN connection<br>2. regular system update and patche | MEDIUM | network administrator |
| R07 | Social engineering | 4 | 2 | Incident response plan | 1. Awareness training<br>2. strong password policy and MFA | MEDIUM | IT securityofficer |
| R08 | server hijacking | 2 | 5 | access control policy | 1. strong server configuration<br>2. effective access control | HIGH | Network administrator |
| R09 | Insider Threat | 5 | 4 | access control policy | 1. effective access control<br>2. strong encryption algorithm | EXTREME | Access control manager |
| R10 | piggybacking | 5 | 1 | access control policy | implement visitor management plan | LOW | Access control manager |
| R11 | Intercepted emails | 3 | 4 | data encryption policy | 1. effective encryption algorithm<br>2. Encrypted databse | HIGH | Access control manager |
| R12 | Data theft | 4 | 5 | Data privacy policy | 1. deactivate email of former staff | EXTREME | Access control manager |

## RISK MATRIX



| | | Consequences | | | | |
|---|---|---|---|---|---|---|
| | | Acceptable level | Bad | Serious | severe | catastrophic |
| | | 1 | 2 | 3 | 4 | 5 |
| Rare | 1 | | | | | |
| Unlikely | 2 | | | R03 | | R08 |
| likely | 3 | | R06 | | R01, R11 | R05 |
| very likely | 4 | | R02, R07 | R04 | R12 | |
| frequent | 5 | R10 | | | R09 | |

## RISK COLOURS AND MEANING

| RISK COLOUR | | DEFINITION |
|---|---|---|
| 🟥 | | EXTREME |
| 🟥 | | HIGH |
| 🟧 | | MIDDLE |
| 🟩 | | LOW |

## GLOSSARY

- **Social engineering**: it’s a manipulative technique used by attackers to gain unauthorized access into a data, system and IT infrastructure.
- **Malware**: is a software intended to cause harm or damage to system, software etc.
- **IP address**: it’s a unique label assigned to each device connected to a computer network for communication,
- **DNS (Domain Name System)** : its essential part of internet infrastructure that allows users to access and communicate with online service.
- **DDOS (Distributed Denial of Service)**: it’s a flood of network traffic on a system or server by bad attackers which deny legitimate users access to the server or system.
- **VPN (Virtual Private Network)**: it’s a secured and private network that users use to access organization data, information by hiding/masking their IP address. It’s a remote network.
- **Piggy theft**: it’s an occurrence where visitor hide/steal data or vital material and put it in a larger container to avoid detection by security.
- **Man-in-the-middle:** it’s a situation where a bad attacker intercept data, information in transit or motion.
- **Segregation of duties:** is when duties and responsibilities are divided and/or shared among multiple employees to prevent fraud, errors etc.

- **RTO (recovery time objective):** it's the time required for business function to be restored after interruption or disruption.
- **IDS/IPS (Intrusion detection system and intrusion prevention system):** They are mechanism put in place to detect, prevent any intrusion into the system.
- **Phishing attack:** it's a form of social engineering whereby bad actors send malicious messages to emails with intention to gain unauthorized access.
- **SSL/TLS (secure socket layer and transport socket layer):** it's a security protocol that verifies that the website is secured to access its content.
- **Privilege abuse:** it's a situation when authorized users wrongfully abuse the privilege given to access data and system which can cause damage to the data or system.
- **Insider threat:** it's a threat that is caused by someone in the organization either by negligence or evil intent.
- **Firewall:** it's a network security system that control network traffic on a system or server based on predetermined rules.
- **RPO (recovery point objective):** it's the point in time at which data can be recovered during disruption. It's the amount of data an organization can tolerate losing within a specified time period.