Risk Description	Risk ID
Cable Damage or Cut in Physical Layer causing loss of connectivity	1
Attacker spoofs MAC addresses to bypass security controls.	2
Use of outdated or weak encryption algorithms exposing data.	3
Attacker forges IP addresses to gain unauthorized access or disrupt communication.	4
Flooding target with TCP connection requests to exhaust resources	5
Unauthorized user takes over a valid session.	6
Injection of malicious SQL queries to manipulate databases	7

Impact
Network downtime and data transmission failure
Unauthorized access to network segments
Data confidentiality breach.
Unauthorized access, network disruption.
Service disruption or denial of service
Data theft or unauthorized actions
Data loss, unauthorized data access

Risk Owner	Related Asset
Network Infrastructure Manager.	Network cables, switches, and physical infrastructure.
Network Security Administrator	Switches, network interface cards (NICs)
IT Security Manager.	Encryption software, communication channels.
Network Operations Manager	Routers, firewalls, IP address management systems
Security Operations Center (SOC) Manager	Network servers and firewalls
Application Security Lead	Session management systems, web servers
Application Development Manager	Database servers, web applications

Risk Treatment Implementor
Network Infrastructure Team Lead
Network Security Engineer
Security Architect / System Admin
Network Security Engineer
SOC Team / Network Security Engineer
Application Security Lead / DevOps
App Development Lead

Probability	Controls
3	Use cable management, protective conduits, and regular inspections.
3	Enable port security on switches and use MAC filtering
2	Upgrade to strong encryption standards (e.g., TLS 1.3)
1	Implement ingress and egress filtering on routers
5	.Deploy DoS mitigation tools and configure rate limiting
3	.Use encrypted session tokens and implement session timeouts
4	Implement input validation and parameterized queries

Risk Treatment Methodolgy	Risk Level	Risk Rate	Impact
Mitigate	🟩	15	5
Mitigate	🟩	9	3
Mitigate	🟩	10	5
Mitigate	🟩	3	3
Mitigate	🟩	25	5
Mitigate	🟩	15	5
Mitigate	🟩	16	4
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	
	🟩	🟩	

ISO 27001 Control
A.11.1.4 Protecting Equipment.
A.13.1.1 Network Controls
A.10.1.1 Cryptographic Controls
A.13.1.1 Network Controls
A.13.1.3 Protection Against Malicious Code
A.10.1 Cryptographic Controls.
A.14.2 Security in Development and Support Processes.

Response Plan
Inspect physical infrastructure regularly/ Quickly replace or repair damaged cables.
Configure port security to limit allowed MAC addresses / Monitor network for suspicious MAC activity.
Audit encryption methods used/ Replace weak algorithms with strong, updated ones.
Configure routers to drop packets with invalid IP addresses/ Audit router configurations regularly
Monitor network traffic for abnormal spikes/ Activate DoS mitigation appliances
Enforce use of HTTPS and secure cookies/ Monitor session activities for anomalies
Conduct secure coding training

Risk Review	Risk Rate	Status
Quarterly physical audits	3	Implemented
Monthly network security audits	1	Partially Implemented
Quarterly encryption assessments	0	Implemented
Quarterly router audits	0	Implemented
Weekly traffic analysis during peak hours	6	Implemented
Monthly session security reviews.	3	Implemented
Bi-monthly application security testing	4	Ongoing

Evidences	Result of Monitoring
Physical audit reports and repair logs	Low Risk (Monitoring)
Switch logs; security audit reports	Low Risk (Monitoring)
Encryption audit reports; configuration files	Low Risk (Monitoring)
Router logs; audit reports	Low Risk (Monitoring)
Traffic monitoring reports; incident logs.	Low Risk (Monitoring)
Security logs; vulnerability scans	Low Risk (Monitoring)
Penetration test reports; code review logs	Low Risk (Monitoring)

0