Procedure for Operational Planning and Implementation of Security Controls

XXXX-ISMS-P10

Approvals

Prepared by: Consulting firm	Review: Quality Manager	Approved by: General Manager
Name:	Name:	Name:
Signature:	Signature:	Signature:

Statement of amendments

NO	Statement of amendments	Date of Amendment	Page number
1.			
2.			
3.			
4.			

Distribution List

NO	Administration	Responsible	Number of copies
1.			
2.			
3.			
4.			

Issue/Revision Number: 01/00 Date of issue: 00/00/2000	Here you put the logo company or office	Procedure for Operational Planning and Implementation of Security Controls XXXX-ISMS-P10

1- Purpose:

This procedure aims to establish a clear and comprehensive methodology for operational planning and implementation of security controls in (write your organization's name here) to ensure:

- **Effective application of all security controls identified in the Statement of Applicability (SoA)**
- **Integration of security controls into daily operational processes across all departments**
- **Management of operational activities in a way that maintains business continuity and information security**
- **Continuous monitoring and evaluation of the effectiveness of implemented controls**

2- Scope:

This procedure applies to all operational activities, including:

- **Operation of IT systems, databases, and applications**
- **Management of user access and permissions**
- **Monitoring daily operations of the information security infrastructure**
- **Implementation of controls related to data, systems, and equipment**
- **Cross-departmental processes linked to information security operations**

3- Responsibilities:

Role	Responsibilities
Top Management	Approves the annual operational security plan and ensures the provision of required resources.
ISMS Management Representative (ISMS MR)	Oversees the planning, implementation, and periodic review of security controls.
Information Security Department	Prepares and executes the operational security plan and monitors performance.
IT Department	Operates systems and enforces all technical controls defined in the SoA.
Process Owners	Integrate applicable security controls within their operational workflows.
All Employees	Comply with operational security procedures and do not exceed authorized access rights.

4- Definitions:

Term	Definition
Security Controls	Technical or administrative measures implemented to protect the confidentiality, integrity, and availability of information.
Operational Security Plan	A document defining operational activities, responsible parties, resources, and schedules for implementing security controls.
SoA (Statement of Applicability)	A document listing selected ISO/IEC 27001 controls and describing their implementation status.

Operational Procedure	A structured sequence of actions ensuring that controls are effectively implemented.

5- Tools and models:

NO	Form name	Code	Retention period	Storage location
1	Annual Operational Security Plan Form	XXXX-ISMS-F31	Annual	Information Security Dept.
2	Daily Security Controls Operation Log	XXXX-ISMS-F32	3 years	Document Management System (DMS)
3	Security Controls Effectiveness Monitoring Form	XXXX-ISMS-F33	3 years	Information Security Dept.
4	Periodic Operational Review Report	XXXX-ISMS-F34	3 years	ISMS Management Representative

6- Procedure Steps:

NO	Step	Detailed Description	Responsible Party	Form Used	Update Responsibility
1	**Define operational security scope**	Identify systems, assets, and processes subject to operational security control.	ISMS MR + Security Dept.	XXXX-ISMS-F31	ISMS MR
2	**Identify applicable security controls**	Review the Statement of Applicability (SoA) to determine which controls must be operationalized.	Security Dept.	XXXX-ISMS-F31	Security Dept.
3	**Prepare the annual operational security plan**	Include daily activities, responsible departments, resources, and timeframes for each control.	Security Dept.	XXXX-ISMS-F31	ISMS MR
4	**Obtain top management approval**	Submit the plan to top management for official approval before implementation.	Top Management	XXXX-ISMS-F31	Top Management
5	**Implement technical controls**	Apply security measures such as encryption, monitoring, access control, and backups.	IT Dept.	XXXX-ISMS-F32	IT Dept.
6	**Implement administrative controls**	Apply administrative measures such as policies, user awareness, and training programs.	Security Dept. + HR Dept.	XXXX-ISMS-F32	Security Dept.

7	**Record daily operational activities**	Document each control's implementation in the operation log.	Security Dept.	XXXX-ISMS-F32	ISMS MR
8	**Monitor operational performance**	Track compliance and performance of implemented controls.	ISMS MR	XXXX-ISMS-F33	ISMS MR
9	**Analyze monitoring results**	Review daily records to detect deviations or incomplete operations.	Security Dept.	XXXX-ISMS-F33	Security Dept.
10	**Address operational deviations**	Identify root causes and implement corrective actions for any deviations.	ISMS MR + Security Dept.	XXXX-ISMS-F33	ISMS MR
11	**Evaluate control effectiveness**	Measure control performance using defined KPIs and report results.	Security Dept.	XXXX-ISMS-F33	Security Dept.
12	**Prepare periodic operational review reports**	Document overall control performance (monthly or quarterly).	ISMS MR	XXXX-ISMS-F34	ISMS MR
13	**Submit reports to top management**	Present performance results during management review meetings.	ISMS MR	XXXX-ISMS-F34	Top Management
14	**Update controls after operational changes**	Revise controls following system or process modifications.	Security Dept.	XXXX-ISMS-F31	ISMS MR
15	**Verify alignment with SoA**	Ensure that each SoA control is actively implemented and regularly reviewed.	ISMS MR	XXXX-ISMS-F33	ISMS MR
16	**Conduct semi-annual operational plan review**	Evaluate plan effectiveness and update where necessary.	ISMS MR + Top Management	XXXX-ISMS-F34	ISMS MR
17	**Continuous improvement**	Recommend improvements and lessons learned to enhance operational control.	Security Dept.	All Forms	ISMS MR

7- Risk management:

Risk	Cause	L×C	Level
Failure to implement some controls	Lack of follow-up or resources	4×4 = 16	High
Incorrect operation of technical controls	Insufficient training or supervision	3×4 = 12	Medium
Delay in updating operational plan	Weak periodic review	3×3 = 9	Medium
Loss of operational records	Poor documentation or backup	2×4 = 8	Medium
Repeated operational incidents	Ineffective control evaluation	3×4 = 12	Medium

8- Key Performance indicators (KPIs):

Indicator	Measurement method	Target	Frequency
Percentage of implemented security controls	(Implemented ÷ Total) × 100	≥ 95 %	Monthly
On-time implementation of operational activities	(Completed on schedule ÷ Total) × 100	≥ 90 %	Quarterly
Number of detected operational deviations	Review of logs	≤ 3	Monthly
Percentage of controls evaluated for effectiveness	(Evaluated ÷ Total) × 100	100 %	Semi-annual

9- References

- **ISO/IEC 27001:2022 – Clause 8 (Operation)**
- **ISO/IEC 27002:2022 – Control 5.36 (Operational Planning and Control)**
- **Statement of Applicability (SoA)**
- **Operational Security Policy (XXXX-ISMS-PL11)**

Section 1: General Information

Item	Details
Date	15 / 03 / 2025
Time Period	☐ Morning ☐ Evening ☐ Night
Executing Department	Information Security Department
Operator Name	Eng. Mohammed Al-Saggaf
Reviewed By	ISMS Management Representative
Page Number	Page 1 of 3

Section 2: Daily Security Control Operations

No.	Security Control	Operational Activity	Actual Results	Status	Corrective Actions / Notes	Responsible Party	Signature	Date
1	Daily Data Backup	Full backup performed for all critical databases	100% Success	✅ Completed	Restoration verified successfully	IT Dept.	.....	15/03/2025
2	System Log Review	Reviewed data center access logs	No unauthorized access detected	✅ Completed	—	InfoSec Dept.	.....	15/03/2025
3	Security Systems Check	Firewall and IDS reviewed	One suspicious IP automatically blocked	⚠ Under Review	Report sent to ISMS MR	InfoSec Dept.	.....	15/03/2025
4	System Updates	Applied security patches to HRMS system	4/4 systems updated	✅ Completed	—	IT Dept.	.....	15/03/2025
5	Antivirus Scan	Updated definitions and ran full system scan	No threats detected	✅ Completed	—	IT Dept.	.....	15/03/2025
6	Email Security	Reviewed alerts from secure mail system	2 messages quarantined	⚠ Monitored	Isolation confirmed	InfoSec Dept.	.....	15/03/2025
7	Server Performance Monitoring	Checked CPU, RAM, and network utilization	All within normal range	✅ Completed	—	IT Dept.	.....	15/03/2025

No.	Security Control	Operational Activity	Actual Results	Status	Corrective Actions / Notes	Responsible Party	Signature	Date
8	Access Control Review	Checked new user access requests	1 pending management approval	⚠ Follow-up	Approval request submitted	HR + InfoSec	.....	15/03/2025

Section 3: Daily Summary

Item	Result
Total activities executed	8
Fully completed	6
Under review	2
General observations	No security incidents reported. One blocked intrusion attempt detected.
Daily risk level	Low
Report submitted to	ISMS Management Representative

Section 4: Recording Instructions

1. This log must be filled out **daily** by the executing department (IT or Information Security).
2. Every security control activity must be recorded (updates, scanning, monitoring, backup, etc.).
3. Use clear status indicators (✅ Completed, ⚠ Under Review, ⛔ Not Done).
4. Report any critical incident immediately to the ISMS Management Representative.
5. Retain this log in the DMS for **three (3) years**.

Review and Approval

Role	Name	Job Title	Signature	Date
Prepared by:		Operator		
Reviewed by:		ISMS Management Representative		
Approved by:		Information Security Director		

Issue/Revision Number: 01/00

Date of issue: 00/00/2000

Here is where the logo goes Company or office

Document register

Information Security Management System

Procedures			
NO	**Procedure**	**Code**	**Forms**
1	Conducting a context analysis and identifying stakeholders	XXXX-ISMS-P01	XXXX-ISMS-F01 XXXX-ISMS-F02
2	Perform and periodically review the scope of the information security management system	XXXX-ISMS-P2	XXXX-ISMS -F03 XXXX-ISMS -F04
3	Leadership and commitment to information security	XXXX-ISMS-P3	XXXX-ISMS -F05 XXXX-ISMS -F06 XXXX-ISMS -F07
4	Procedure for determining roles, responsibilities, and authorities in the information security management system	XXXX-ISMS-P4	XXXX-ISMS -F08 XXXX-ISMS -F09 XXXX-ISMS -F010
5	Information Security Risk Identification, Assessment, and Treatment Procedure	XXXX-ISMS-P5	XXXX-ISMS -F11 XXXX-ISMS -F12 XXXX-ISMS -F13
6	Identification, monitoring, and analysis of security objectives	XXXX-ISMS-P6	XXXX-ISMS -F14 XXXX-ISMS -F15 XXXX-ISMS -F16
7	Information Security Training and Awareness Management Procedure	XXXX-ISMS-P7	XXXX-ISMS -F17 XXXX-ISMS -F18 XXXX-ISMS -F19 XXXX-ISMS -F20 XXXX-ISMS -F21 XXXX-ISMS -F22
8	Internal and external security communication and liaison procedures	XXXX-ISMS-P8	XXXX-ISMS -F23 XXXX-ISMS -F24 XXXX-ISMS -F25 XXXX-ISMS -F26
9	Procedure for creating, adjusting, updating, modifying, and storing documents and records	XXXX-ISMS-P9	XXXX-ISMS -F27 XXXX-ISMS -F28 XXXX-ISMS -F29 XXXX-ISMS -F30
10	Operational planning and implementation of security controls	XXXX-ISMS-P10	XXXX-ISMS -F31 XXXX-ISMS -F32

			XXXX-ISMS -F33 XXXX-ISMS -F34
11	Security Incident Management and Response Procedure	XXXX-ISMS-P11	XXXX-ISMS -F35 XXXX-ISMS -F36 XXXX-ISMS -F37 XXXX-ISMS -F38
12	Conducting Security Change Assessment and Management	XXXX-ISMS-P12	XXXX-ISMS -F39 XXXX-ISMS -F40 XXXX-ISMS -F41
13	Asset classification and risk assessment procedure	XXXX-ISMS-P13	XXXX-ISMS -F42 XXXX-ISMS-F43 XXXX-ISMS-F44
14	Information Security Supplier and Contract Management Procedure	XXXX-ISMS-P14	XXXX-ISMS-F45 XXXX-ISMS-F46 XXXX-ISMS -F47 XXXX-ISMS -F48 XXXX-ISMS -F49 XXXX-ISMS -F50
15	Authority Management and Account Protection Procedure	XXXX-ISMS-P15	XXXX-ISMS -F51 XXXX-ISMS -F52 XXXX-ISMS -F53 XXXX-ISMS -F54 XXXX-ISMS -F55
16	Monitoring, measurement, and analysis of security performance	XXXX-ISMS-P16	XXXX-ISMS -F56 XXXX-ISMS -F57 XXXX-ISMS -F58 XXXX-ISMS -F59 XXXX-ISMS -F60
17	Internal audit procedure for the information security management system	XXXX-ISMS-P17	XXXX-ISMS -F61 XXXX-ISMS -F62 XXXX-ISMS -F63 XXXX-ISMS -F64 XXXX-ISMS -F65
18	Management Review Procedure – Information Security Management System	XXXX-ISMS-P18	XXXX-ISMS -F66 XXXX-ISMS -F67 XXXX-ISMS -F68 XXXX-ISMS -F69

Issue/Revision Number: 01/00

Date of issue: 00/00/2000

Here is where the logo goes Company or office

Document register

Information Security Management System

19	Non-conformity management and corrective action procedure Information security management system	XXXX-ISMS-P19	XXXX-ISMS -F70 XXXX-ISMS-F71
20	Continuous Improvement Procedure – Information Security Management System	XXXX-ISMS-P20	XXXX-ISMS -F72 XXXX-ISMS-F73
21	Implementation and updating of the security governance framework	XXXX-ISMS-P21	XXXX-ISMS -F74 XXXX-ISMS -F75 XXXX-ISMS -F76 XXXX-ISMS -F77 XXXX-ISMS -F78
22	Procedure for the distribution of security responsibilities and tasks	XXXX-ISMS-P22	XXXX-ISMS -F79 XXXX-ISMS -F80 XXXX-ISMS -F81 XXXX-ISMS -F82 XXXX-ISMS -F83
23	Implementation of sensitive task separation	XXXX-ISMS-P23	XXXX-ISMS -F84 XXXX-ISMS -F85 XXXX-ISMS -F86 XXXX-ISMS -F87 XXXX-ISMS -F88
24	Review of legal obligations, confidentiality obligations, and data protection	XXXX-ISMS-P24	XXXX-ISMS -F89 XXXX-ISMS -F90 XXXX-ISMS -F91 XXXX-ISMS -F92
25	Integrating information security into the project life cycle	XXXX-ISMS-P25	XXXX-ISMS-F93 XXXX-ISMS-F94 XXXX-ISMS -F95 XXXX-ISMS -F96
26	Conducting Security Assessments of Suppliers and Partners	XXXX-ISMS-P26	XXXX-ISMS -F97 XXXX-ISMS -F98 XXXX-ISMS -F99 XXXX-ISMS -F100
27	Monitoring and controlling security throughout the supply chain	XXXX-ISMS-P27	XXXX-ISMS -F101 XXXX-ISMS -F102 XXXX-ISMS -F103 XXXX-ISMS -F104
28	Conducting an assessment of the impact of changes on information security	XXXX-ISMS-P28	XXXX-ISMS -F105 XXXX-ISMS -F106 XXXX-ISMS -F107

Issue/Revision Number: 01/00

Date of issue: 00/00/2000

Here is where the logo goes Company or office

Document register

Information Security Management System

29	Cloud Security Management Procedure	XXXX-ISMS-P29	XXXX-ISMS-F108 XXXX-ISMS-F109 XXXX-ISMS-F110
30	Developing and testing business continuity plans	XXXX-ISMS-P30	XXXX-ISMS -F111 XXXX-ISMS -F112 XXXX-ISMS -F113
31	Legal Records and Information Retention Procedure	XXXX-ISMS-P31	XXXX-ISMS -F114 XXXX-ISMS -F115 XXXX-ISMS -F116
32	Information Security Management Procedure in the Employee Life Cycle	XXXX-ISMS-P32	XXXX-ISMS -F117 XXXX-ISMS -F118 XXXX-ISMS -F119 XXXX-ISMS -F120
33	Conducting background checks	XXXX-ISMS-P33	XXXX-ISMS -F121 XXXX-ISMS -F122
34	Implementation of mandatory security training programs	XXXX-ISMS-P34	XXXX-ISMS-F123 XXXX-ISMS -F124 XXXX-ISMS -F125 XXXX-ISMS -F126
35	Follow-up procedure for compliance with safe use of assets	XXXX-ISMS-P35	XXXX-ISMS -F127 XXXX-ISMS -F128 XXXX-ISMS -F129
36	Procedure for Terminating Employee Powers and Returning Assets	XXXX-ISMS-P36	XXXX-ISMS -F130 XXXX-ISMS -F131 XXXX-ISMS -F132 XXXX-ISMS -F133
37	Physical Access Control and Facility Protection Procedure	XXXX-ISMS-P37	XXXX-ISMS -F134 XXXX-ISMS -F135 XXXX-ISMS -F136 XXXX-ISMS -F137 XXXX-ISMS -F138
38	Access Card Management and Surveillance Systems Procedure	XXXX-ISMS-P38	XXXX-ISMS-F139 XXXX-ISMS-F140 XXXX-ISMS -F141 XXXX-ISMS -F142 XXXX-ISMS -F143
39	Protecting equipment during use and storage	XXXX-ISMS-P39	XXXX-ISMS -F144 XXXX-ISMS -F145

			XXXX-ISMS -F146 XXXX-ISMS -F147
40	Asset Protection Procedure During Use, Transport, and Storage	XXXX-ISMS-P40	XXXX-ISMS -F148 XXXX-ISMS -F149 XXXX-ISMS -F150 XXXX-ISMS -F151
41	Procedure for the secure destruction of data and equipment	XXXX-ISMS-P41	XXXX-ISMS -F152 XXXX-ISMS -F153 XXXX-ISMS -F154 XXXX-ISMS -F155
42	Implementation of security controls for remote workers	XXXX-ISMS-P42	XXXX-ISMS-F156 XXXX-ISMS -F157 XXXX-ISMS -F158 XXXX-ISMS -F159
43	Procedure for managing and controlling the security of mobile devices owned by the facility	XXXX-ISMS-P43	XXXX-ISMS -F160 XXXX-ISMS -F161 XXXX-ISMS -F162 XXXX-ISMS -F163
44	Procedure for using personal devices and ensuring their compliance with security controls	XXXX-ISMS-P44	XXXX-ISMS -F164 XXXX-ISMS -F165 XXXX-ISMS -F166 XXXX-ISMS -F167
45	Conducting an asset inventory and updating its security record	XXXX-ISMS-P45	XXXX-ISMS -F168 XXXX-ISMS -F169 XXXX-ISMS -F170 XXXX-ISMS -F171 XXXX-ISMS -F172
46	Account Management and Authorization Procedure	XXXX-ISMS-P46	XXXX-ISMS -F173 XXXX-ISMS -F174 XXXX-ISMS -F175 XXXX-ISMS -F176
47	Encryption Key Management Procedure and Implementation	XXXX-ISMS-P47	XXXX-ISMS -F177 XXXX-ISMS -F178 XXXX-ISMS -F179 XXXX-ISMS -F180 XXXX-ISMS -F181
48	Monitoring of operating systems and software	XXXX-ISMS-P48	XXXX-ISMS -F182 XXXX-ISMS -F183 XXXX-ISMS -F184 XXXX-ISMS -F185
49	Periodic backup and restore testing	XXXX-ISMS-P49	XXXX-ISMS -F186 XXXX-ISMS -F187

			XXXX-ISMS -F188 XXXX-ISMS -F189 XXXX-ISMS -F190
50	Access control and security log analysis	XXXX-ISMS-P50	XXXX-ISMS -F191 XXXX-ISMS -F192 XXXX-ISMS -F193
51	Network and Email Security Management Procedure	XXXX-ISMS-P51	XXXX-ISMS -F194 XXXX-ISMS-F195 XXXX-ISMS -F196 XXXX-ISMS -F197
52	Performing vulnerability assessments and implementing security updates	XXXX-ISMS-P52	XXXX-ISMS -F198 XXXX-ISMS -F199 XXXX-ISMS -F200 XXXX-ISMS -F201
53	Secure Development Lifecycle Procedure	XXXX-ISMS-P53	XXXX-ISMS -F202 XXXX-ISMS -F203 XXXX-ISMS -F204 XXXX-ISMS -F205 XXXX-ISMS -F206
54	Security Procedure for Development and Testing Environments	XXXX-ISMS-P54	XXXX-ISMS -F207 XXXX-ISMS -F208 XXXX-ISMS -F209 XXXX-ISMS-F210
55	Virus and malware scanning and control	XXXX-ISMS-P55	XXXX-ISMS -F211 XXXX-ISMS -F212 XXXX-ISMS -F213 XXXX-ISMS -F214
56	Security Incident Reporting and Root Cause Analysis Procedure	XXXX-ISMS-P56	XXXX-ISMS -F215 XXXX-ISMS -F216 XXXX-ISMS -F217 XXXX-ISMS -F218 XXXX-ISMS -F219
57	Risk Management Procedure for Emerging Technologies	XXXX-ISMS-P57	XXXX-ISMS-F220 XXXX-ISMS-F221 XXXX-ISMS -F222 XXXX-ISMS -F223

Issue/Revision Number: 01/00

Date of issue: 00/00/2000

Here is where the logo goes Company or office

Document register

Information Security Management System

58	Email and Digital Communications Security Management and Control Procedure	XXXX-ISMS-P58	XXXX-ISMS -F224 XXXX-ISMS -F225 XXXX-ISMS -F226 XXXX-ISMS -F227
59	Procedure for preparing and approving email disclaimers	XXXX-ISMS-P59	XXXX-ISMS -F228

Policies

NO	Policy	Code
1	Context Analysis and Stakeholder Identification Policy	XXXX-ISMS-PL01
2	Information Security Management System Scope Definition Policy	XXXX-ISMS-PL02
3	General Information Security Policy	XXXX-ISMS-PL03
4	Policy on roles, responsibilities, and authorities in information security	XXXX-ISMS-PL04
5	Information Security Risk and Opportunity Management Policy	XXXX-ISMS-PL05
6	Security Objectives and Measurement Policy	XXXX-ISMS-PL06
7	Information Security Competence, Training, and Awareness Policy	XXXX-ISMS-PL07
8	Internal and External Communication Policy for Information Security	XXXX-ISMS-PL08
9	Information Security Document and Record Control Policy	XXXX-ISMS-PL09
10	Secure Systems Operation Policy	XXXX-ISMS-PL10
11	Security Incident Response Policy	XXXX-ISMS-PL11
12	Information Security Management System Change Policy	XXXX-ISMS-PL12
13	Information Asset Security Policy	XXXX-ISMS-PL13
14	Supplier Information Security Policy	XXXX-ISMS-PL14
15	Access Control Policy	XXXX-ISMS-PL15
16	Monitoring, Measurement, Analysis, and Evaluation Policy	XXXX-ISMS-PL16
17	Internal Audit Policy	XXXX-ISMS-PL17
18	Management Review Policy	XXXX-ISMS-PL18
19	Non-Conformity Handling and Corrective Action Policy	XXXX-ISMS-PL19

Issue/Revision Number: 01/00

Date of issue: 00/00/2000

Here is where the logo goes Company or office

Document register

Information Security Management System

20	Continuous Improvement Policy for the Information Security Management System	XXXX-ISMS-PL20
21	Information Security Governance Policy	XXXX-ISMS-PL21
22	Segregation of Duties Policy	XXXX-ISMS-PL22
23	Duty Separation Policy	XXXX-ISMS-PL23
24	Legal and Regulatory Compliance Policy for Information Security	XXXX-ISMS-PL24
25	Information Security Policy for Projects	XXXX-ISMS-PL25
26	Information Security in External Party Relationships Policy	XXXX-ISMS-PL26
27	Supply Chain Information Security Policy	XXXX-ISMS-PL27
28	Security Change Management Policy	XXXX-ISMS-PL28
29	Cloud Computing Security Policy	XXXX-ISMS-PL29
30	Information Security Continuity Policy	XXXX-ISMS-PL30
31	Legal Records and Evidence Management Policy	XXXX-ISMS-PL31
32	Personnel Security Policy – Before, During, and After Employment	XXXX-ISMS-PL32
33	Pre-Employment Security Verification Policy	XXXX-ISMS-PL33
34	Information Security Awareness and Training Policy	XXXX-ISMS-PL34
35	Information Security Behavior and Responsibility Policy	XXXX-ISMS-PL35
36	Termination or Change of Employment Security Policy	XXXX-ISMS-PL36
37	Physical and Environmental Security Policy	XXXX-ISMS-PL37
38	Physical Access Control Policy	XXXX-ISMS-PL38
39	Equipment and Media Protection Policy	XXXX-ISMS-PL39
40	Secure Disposal of Assets Policy	XXXX-ISMS-PL40
41	Remote Working and Shared Office Policy	XXXX-ISMS-PL41
42	Facility-Owned Mobile Device Security Policy	XXXX-ISMS-PL42
43	Personal Device Use at Work Policy	XXXX-ISMS-PL43
44	Technical Asset Management Policy	XXXX-ISMS-PL44
45	Access and Authentication Management Policy	XXXX-ISMS-PL45
46	Encryption and Data Protection Policy	XXXX-ISMS-PL46
47	Operational Security and Servers Policy	XXXX-ISMS-PL47
48	Data Backup and Recovery Policy	XXXX-ISMS-PL48
49	Monitoring and Log Analysis Policy	XXXX-ISMS-PL49
50	Network and Communications Security Policy	XXXX-ISMS-PL50
51	Vulnerability Management Policy	XXXX-ISMS-PL51
52	Secure System Development Policy	XXXX-ISMS-PL52
53	Test Environment Isolation Policy	XXXX-ISMS-PL53
54	Malware Protection Policy	XXXX-ISMS-PL54
55	Information Security Incident Management Policy	XXXX-ISMS-PL55

56	**Emerging Technologies and Artificial Intelligence Policy**	**XXXX-ISMS-PL56**
5	**Email and Electronic Communication Security Policy**	**XXXX-ISMS-PL57**