جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

General Cybersecurity policy

Version: 2.0

CODE: DICT.I.06-01.CS.E.V2.0

1 Table of Con.

2 Intellectual Property Information

This document is the intellectual property of the Deanship of Information and Communication Technology (DICT) at Imam Abdulrahman bin Faisal university (IAU). The content of this document is intended solely for authorized recipients. Any distribution, disclosure, publication, or copying of this document without written permission from DICT is strictly prohibited.

3 Document Control

3.1 Information

Title	Classification	Version	Status
GENERAL CYBERSECURITY POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)/Reviewers	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	01/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	02/03/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	16/12/2023	REVIEW AND UPDATE

3.3 Document Review

Date of Next Scheduled Review
01/01/2025

3.4 Distribution List

#	Recipients
1	ALL DICT DEPARTMENTS
2	LEGAL AFFAIRS
3	IAU WEBSITE
4	

3.5 Approval

Name	Position Title	Decision Number	Date
DR. NIHAD AL-OMAIR	VICE PRESIDENT OF DEVELOPMENT AND COMMUNITY PARTNERSHIP	61945	06/03/2024

4 Introduction

The university has established the Cybersecurity Management to work on developing and managing operations to protect its data and assets, as well as to safeguard personal data, given its importance in ensuring the successful continuity of the university's operations. This document outlines the policy within the university and security requirements based on best practices, standards, and regulations applicable in this field.

This policy is included within the framework of the university's policies and falls under the authority granted by the governing body starting from the date of its adoption.

5 Policy Objective

The Cybersecurity Policy defines the systems and provisions that maintain the security and confidentiality of data and the technical infrastructure of the university. All data and information technology assets are necessary for the university's operations and contribute to achieving its strategic objectives. Therefore, governing this data, protecting its confidentiality, integrity, and availability is essential. The Cybersecurity Policy aims to protect the university's assets from threats and effectively mitigate risks.

The provisions of this policy are applied in accordance with the national data governance policies issued by the National Data Management Office (NDMO) and the requirements of the National Cybersecurity Authority (NCA), which include the foundational cybersecurity controls, personal data protection system, ISO 27001 standard, National Institute of Standards and Technology (NIST) standards, and internationally recognized best practices in the field.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals working within the university, whether through permanent or temporary contracts, both directly and indirectly, including suppliers, external contractors, and anyone with permanent or temporary access rights to university data, regardless of its source, form, or nature, as well as to systems, devices, and university databases.

7 Policy

7.1 General Policy Requirements

7.1.1 Data and information technology assets must be protected from leakage, unauthorized access, and threats, whether internal or external, intentional or unintentional.

7.1.2 The documents of cybersecurity must be maintained, along with supporting documents that enable the preparation and implementation of cybersecurity policies within the university. These documents should encompass policies, procedures, standards, and guidelines related to security risks and assessments.

7.1.3 The Cybersecurity Management should develop policies, procedures, standards, and responsibilities for cybersecurity in accordance with global systems, regulations, legislations, and best practices, and these should be disseminated or published and adhered to. They must be applied by all individuals within the university and external/contractual parties, each in their respective domains.

7.1.4 Document tracking should be controlled using version information, document dates, and review details, if applicable.

7.1.5 Effective means of communication should be used to disseminate cybersecurity policies within the university.

7.1.6 All documents related to cybersecurity policies must be reviewed by relevant departments, updated periodically or as needed, or when legislative and regulatory requirements change.

7.1.7 Information must be handled according to specified classifications and in alignment with data classification and data protection policies within the university, ensuring the confidentiality, integrity, and availability of information.

7.1.8 Violation of rights of any individual, copyright-protected company, patent, or any other intellectual property, or similar laws or regulations, is prohibited. This includes, but is not limited to, the installation of unauthorized or unlawful software.

8 Cybersecurity Methodology

8.1.1 The Cybersecurity Management must apply an effective (Plan-Do-Check-Act) methodology in identifying, preparing, monitoring, maintaining, and continuously improving cybersecurity controls and procedures.

8.1.2 The Planning phase (Plan) focuses on identifying and evaluating cybersecurity risks, as well as determining processing controls to manage risks.

8.1.3 The Implementation phase (Do) emphasizes deploying controls and executing risk treatment plans to mitigate and manage risks.

8.1.4 The Checking phase (Check) involves conducting cybersecurity audits within the university, further monitoring, reviewing, and updating the tools used for this purpose to ensure compliance with legal, regulatory, or contractual obligations.

8.1.5 The Acting phase (Act) focuses on modifying cybersecurity controls and procedures within the university and continuously improving them.

9 Principles of Cybersecurity

9.1.1 Data confidentiality, integrity, and availability must be maintained, and necessary controls should be established to allow the use, access, and disclosure of this information in accordance with relevant systems, regulations, legislations, and global best practices.

9.1.2 The policies of cybersecurity within the university are based on the following general principles:

- **Confidentiality**: Ensuring that data is only accessed by authorized individuals, and adequately protecting both confidential and personal data.
- **Integrity**: Ensuring the accuracy and completeness of data and the associated data processing methods.
- **Availability**: Ensuring authorized users can access data, assets, or associated systems in a timely manner when necessary.

9.1.3 The requirements of cybersecurity shall be achieved by enforcing a suitable set of controls by the Cybersecurity Management. These controls must be implemented and reviewed as needed to achieve the university's cybersecurity objectives.

10 Leadership and Commitment towards Cybersecurity

10.1.1 The Cybersecurity Management shall maintain records that demonstrate their commitment to cybersecurity controls, their implementation, activation, monitoring, review, and preservation. This should be achieved through:

10.1.2 Developing cybersecurity policies, standards, and procedures in alignment with regulatory and legislative requirements, in addition to the strategic objectives of the university.

10.1.3 Establishing a mechanism to ensure the university complies with the requirements of the National Cybersecurity Authority, ISO 27001 standard, as well as the requirements of the National Data Management Office and related provisions of the Personal Data Protection system.

10.1.4 Defining roles and responsibilities to achieve the objectives of cybersecurity within the university, periodically reviewing these roles and responsibilities or as needed, and when changes occur in legislative and regulatory requirements.

10.1.5 The Cybersecurity Management shall achieve cybersecurity objectives for the university, in accordance with cybersecurity policies and the university's responsibilities under relevant regulatory provisions and regulations, continuously reviewing and improving them.

10.1.6 Providing sufficient resources for the preparation, implementation, activation, monitoring, review, improvement, and preservation of cybersecurity practices.

10.1.7 Guiding and supporting participants, whether they are affiliates within the university or external parties (contractors/other entities), in the implementation of cybersecurity policies, and providing necessary support.

10.1.8 Defining procedures and standards for managing and assessing cybersecurity risk and threat levels, regularly reviewing them or as needed, and when changes occur in legislative and regulatory requirements.

10.1.9 Ensuring internal audits for cybersecurity are conducted.

10.1.10 Taking corrective actions based on the results of internal audits, security incidents, and external audits, to ensure continuous improvement and ensure that cybersecurity practices achieve the desired results.

11 Cybersecurity Program

11.1.1 The Cybersecurity Management must establish procedures and standards for cybersecurity and document its policies and programs based on the results of the cybersecurity risk assessment. This should ensure the dissemination of cybersecurity requirements and the university's commitment to them, in accordance with the university's organizational business requirements, as well as relevant legislative and regulatory requirements. The approval of these documents must be obtained from the authorized party within the university. Relevant personnel within the university must be informed and committed to these documents.

11.2 Cybersecurity programs encompass a range of domains, including the following key areas:

11.2.1 Cybersecurity Strategy

Aims to ensure the execution of action plans, initiatives, and projects related to cybersecurity in accordance with the approved strategic objectives, legislative and regulatory requirements, and relevant legal provisions and regulations.

11.2.2 Cybersecurity Risk Management

Systematic management of cybersecurity risks to ensure the protection of information, data, and technological assets in line with approved objectives, policies, legislative and regulatory requirements, as well as relevant legal provisions and regulations.

11.2.3 Data Protection

Preservation of information security, data confidentiality, and the safeguarding of personal data to ensure their integrity, safety, accuracy, and availability, in accordance with approved objectives, policies, legislative and regulatory requirements, as well as relevant legal provisions and regulations.

11.2.4 Access Control Management

Enhance information security by implementing specific controls for data access and the use of information technology assets. Prevent unauthorized access and restrict access to the necessary level for performing tasks and activities relevant to the University's operations.

11.2.5 Event Logging and Cybersecurity Monitoring

Regulate the collection, analysis, and real-time monitoring of cybersecurity event logs. This is done to proactively anticipate, detect, and effectively manage cyber-attacks, thereby minimizing potential negative impacts on data or the University's operations.

11.2.6 Cybersecurity Incident and Threat Management

Empower the cybersecurity management to proactively anticipate, detect, and timely identify cybersecurity incidents. Efficiently manage these incidents and address cybersecurity attacks or threats, aiming to minimize potential negative impacts on data or the University's operations. This should be carried out in accordance with legislative and regulatory requirements.

11.2.7 Compliance with Cybersecurity

Monitor violations of non-compliance with cybersecurity controls and requirements. This includes any breaches of policies, applicable standards, regulatory provisions, or relevant regulations. Address these violations in accordance with approved policies, standards, and procedures to ensure continuous improvement of cybersecurity practices within the University.

11.2.8 Cybersecurity Training and Awareness

- This program aims to increase awareness among university affiliates, enhance their understanding of their responsibilities in the field of cybersecurity, develop their skills, and provide necessary awareness programs. This ensures they fulfil their duties in protecting the informational and technological assets of the University.
- Continuous improvement of awareness among university affiliates should be a primary initiative toward enhancing the overall quality of cybersecurity.
- User awareness should be assessed based on appropriate evaluation methods provided by the cybersecurity management.
- The cybersecurity awareness program within the University should cover the following:
    - Safe use, maintenance, and protection of devices used for remote work.
    - Secure handling of login credentials and passwords.
    - Protection of data stored on devices used for remote work, based on their classification and the University's procedures and policies.
    - Secure use of applications and solutions for remote work, such as virtual meetings, collaboration, and file sharing.
    - Secure handling of home networks and ensuring their security settings.
    - Avoiding remote work using untrusted public devices or networks or while being in public places.
    - Unauthorized physical access, loss, and sabotage of technological assets and remote work systems.
    - Direct communication with the cybersecurity management in case of suspected cybersecurity threats.

12 Roles and Responsibilities

The Cybersecurity Management responsibilities:

12.1.1 The Head of Cybersecurity Management is responsible for endorsing the policy by the authorized entity and ensuring its implementation.

12.1.2 The Head of Cybersecurity Management is responsible for endorsing the standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the University's operations.

12.1.3 The Head of Cybersecurity Management may recommend the establishment of a supervisory committee for cybersecurity, with the CISO being one of its members.

12.1.4 The Head of Cybersecurity Management is responsible for ensuring the alignment of this policy with the University's operations.

12.1.5 The Head of Cybersecurity Management is responsible for resolving any conflicts arising from this policy.

12.1.6 The Head of Cybersecurity Management is responsible for providing necessary resources to identify, procure, and implement technical solutions, if possible, to fulfil the policy's requirements.

12.1.7 staff of the Cybersecurity Management should ensure the dissemination of the cybersecurity compliance policy across all departments, staff, and users of the university who are authorized to access technological and information assets.

12.1.8 Staff of the Cybersecurity Management should review the policy periodically according to the established timeline.

The Director of Legal Affairs shall:

12.1.9 Ensure that all cybersecurity policies align with current practices within the university and comply with legislative, regulatory, statutory provisions, and legal obligations.

12.1.10 Ensure that the terms and requirements of cybersecurity, information confidentiality, and personal data protection mentioned in confidentiality undertakings and contracts of university affiliates and external parties/contractors are legally binding.

The Head of Quality Assurance Department shall:

12.1.11 Conduct periodic reviews of the implementation of cybersecurity controls in accordance with the generally accepted standards for review and auditing, legislative and regulatory requirements, and relevant regulatory provisions.

The Dean of Deanship of Human Resources shall:

12.1.12 Implement the requirements of the Human Resources Security Policy.

Top Management, Heads of Departments, Heads of Units, and Advisers shall:

12.1.13 Ensure that all affiliates within the department acknowledge reading and understanding the cybersecurity policies.

12.1.14 Enhance the level of commitment and compliance among all affiliates with the university's cybersecurity policies.

12.1.15 Ensure that all university affiliates must comply with the provisions of this policy and report any security incidents or non-compliance with any provisions outlined in this policy to the Head of Cybersecurity Management.

13 Exceptions

- Deviating from cybersecurity policies, standards, and procedures without obtaining prior official authorization from the Head of Cybersecurity Management is prohibited, unless it conflicts with legislative, regulatory requirements, or relevant regulatory provisions.
- In cases of urgent need for exemption from responsibilities within a cybersecurity policy with no applicable and secure alternative, an exemption request must be submitted to the Head of Cybersecurity Management, including reasons for and duration of the need for the exemption, along with a detailed description of scope and justifications.
- The Cybersecurity Management shall review the request, identify risks, and propose additional controls according to the approved methodology for managing cybersecurity risks in the university. The requestor may be required to approve identified risks and additional controls if necessary.
- The Cybersecurity Management may consult relevant internal and external entities for legal and regulatory matters.

- All cybersecurity exceptions are documented, and the Cybersecurity Oversight Committee is notified of all exemption requests.
- The Cybersecurity Management holds the authority to revoke exceptions once the reasons necessitating them have ceased.

14 Ownership of the Policy

The Head of Cybersecurity Management of the university is responsible for this policy.

15 Policy Changes

Any changes to this policy must be reviewed at least annually or when there are changes in legislative and regulatory requirements. Changes should be documented and approved by the authorized party within the university.

16 Compliance

All individuals within the University, including external parties/contractors, must adhere to the provisions of this policy. The Head of Cybersecurity Management within the university must ensure continuous monitoring of compliance and submit necessary reports on this matter to the authorized party periodically.

Necessary actions must be taken to ensure compliance with the provisions of this policy. This can be achieved through periodic reviews conducted by the Cybersecurity Management or relevant departments. Corrective actions should be taken by the authorized party within the university based on recommendations provided by the Head of Cybersecurity Management regarding any violations of this policy. Disciplinary actions, commensurate with the severity of the incident as determined by the investigation, should be implemented. Examples of disciplinary actions include, but are not limited to:

- Revoking access to data and information **technology** assets and systems connected to the university.
- Issuing a written warning, or terminating the **employment** of the individual, or taking appropriate actions as deemed suitable by the university.

Non-compliance with any provisions of this policy without obtaining prior exemption from the Cybersecurity Management necessitates appropriate actions according to the policies and regulations in place within the university, or as deemed appropriate, and in accordance with contractual terms with any individuals or entities contracted with.

17 Related Policies, Standards and Procedures

- DICT.I.06-02.CS.E.V2.0 - Cybersecurity Compliance Policy.
- DICT.I.06-24.CS.E.V2.0 - Cybersecurity Risk Management Policy
- DICT.I.06-28.CS.E.V2.0 - Cybersecurity Continuity of Business Policy
- DICT.I.06-25.CS.E.V2.0 - Human Resources Security Policy
- DICT.I.06-41.CS.E.V2.0 - Third Party and Suppliers Security Policy
- DICT.I.06-32.CS.E.V2.0 - Physical and Environmental Security Policy
- DICT.I.06-03.CS.E.V2.0 - Data Protection Policy
- DICT.I.06-20.CS.E.V2.0 - Data Storage and Retention Policy
- DICT.I.06-21.CS.E.V2.0 - Data Classification Policy
- DICT.I.06-13.CS.E.V2.0 - Personal Data Protection Policy
- DICT.I.06-29.CS.E.V2.0 - Encryption Policy
- DICT.I.06-39.CS.E.V2.0 - Network Security Policy
- DICT.I.06-09.CS.E.V2.0 - Cybersecurity Incident Management Policy
- DICT.I.06-10.CS.E.V2.0 - Event Logs Management and Cybersecurity Monitoring Policy
- DICT.I.06-05.CS.E.V2.0 - Vulnerability Management and Penetration Testing Policy
- DICT.I.06-30.CS.E.V2.0 - Anti-Malware Policy
- DICT.I.06-42.CS.E.V2.0 - Workstations, Mobile Devices and BYOD Security Policy
- DICT.I.06-43.CS.E.V2.0 - Cloud Computing Security Policy
- DICT.I.06-22.CS.E.V2.0 - System Acquisition, Development, and Maintenance Policy
- DICT.I.06-07.CS.E.V2.0 - Backup and Restoration policy
- DICT.I.06-08.CS.E.V2.0 - Patch and Update Management Policy
- DICT.I.06-26.CS.E.V2.0 - Clear Desk and Clear Screen Policy
- DICT.I.06-04.CS.E.V2.0 - Asset Management Policy
- DICT.I.06-06.CS.E.V2.0 - Change Management Policy
- DICT.I.06-27.CS.E.V2.0 - Acceptable Use of Assets Policy
- DICT.I.06-33.CS.E.V2.0 - Access Control Policy
- DICT.I.06-44.CS.E.V2.0 - Email Security Policy
- DICT.I.06-15.CS.E.V2.0 - Password Management policy
- DICT.I.06-14.CS.E.V2.0 - Web Application Security Policy
- DICT.I.06-12.CS.E.V2.0 - Cookie Policy
- DICT.I.06-38.CS.E.V2.0 - Configuration and Hardening Policy

- DICT.I.06-34.CS.E.V2.0 - Cybersecurity Policy for Project Management
- DICT.I.06-11.CS.E.V2.0 - Data Sharing Policy
- DICT.I.06-37.CS.E.V2.0 - Cybersecurity Policy for Teleworking
- DICT.I.06-40.CS.E.V2.0 - Operations Security Policy
- DICT.I.06-39s.CS.E.V2.0 - Network Security policy
- DICT.I.06-35.CS.E.V2.0 - Cybersecurity Policy for Social Media Accounts and Media
- DICT.I.06-36.CS.E.V2.0 - Cybersecurity Policy to Protect Printers, Scanners and Photocopiers
- DICT.I.06-45.CS.E.V2.0 Cybersecurity assessment and audit policy
- DICT.I.06-46.CS.E.V2.0 Storage Media Security Policy
- DICT.I.06-47.CS.E.V2.0 Secure Systems Development Life Cycle policy
- DICT.I.06-48.CS.E.V2.0 Privileged Access Workstations Standards
- DICT.I.06-49.CS.E.V2.0 Identity And Access Management Standards
- DICT.I.06-50.CS.E.V2.0 Physical Security Standards
- DICT.I.06-51.CS.E.V2.0 Secure Coding Standard
- DICT.I.06-52.CS.E.V2.0 Advanced Persistent Threats (APT) Standards
- DICT.I.06-53.CS.E.V2.0 Data Loss Prevention Standards
- DICT.I.06-54.CS.E.V2.0 Network Detection and Response Standards
- DICT.I.06-55.CS.E.V2.0 Email Protection Standards
- DICT.I.06-56.CS.E.V2.0 Data Cybersecurity Standards
- DICT.I.06-57.CS.E.V2.0 Standard Virtualization Security
- DICT.I.06-58.CS.E.V2.0 Database Security Standards
- DICT.I.06-59.CS.E.V2.0 Social Media Security Standard
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards
- DICT.I.06-61.CS.E.V2.0 Data Protection Standards
- DICT.I.06-62.CS.E.V2.0 Asset Management Standards
- DICT.I.06-63.CS.E.V2.0 Vulnerability Management and Penetration Testing Standards
- DICT.I.06-64.CS.E.V2.0 Change Management Standards
- DICT.I.06-65.CS.E.V2.0 Backup and Restoration Standards
- DICT.I.06-66.CS.E.V2.0 Patch Management Standards
- DICT.I.06-67.CS.E.V2.0 Cybersecurity Incident Management Standards
- DICT.I.06-68.CS.E.V2.0 Cybersecurity Events Logs and Monitoring Management standards
- DICT.I.06-69.CS.E.V2.0 Password Management standards

- DICT.I.06-70.CS.E.V2.0 System Acquisition, Development and Maintenance Standards
- DICT.I.06-71.CS.E.V2.0 Encryption Standards
- DICT.I.06-72.CS.E.V2.0 Anti-Malware Standards
- DICT.I.06-73.CS.E.V2.0 Web Application Security Standards
- DICT.I.06-74.CS.E.V2.0 Cybersecurity Policy for Project Management Standards
- DICT.I.06-75.CS.E.V2.0 Configuration and Hardening Standards
- DICT.I.06-76.CS.E.V2.0 Server Security Standards
- DICT.I.06-77.CS.E.V2.0 Network Security Standards
- DICT.I.06-78.CS.E.V2.0 Third Party and Suppliers Security Standards
- DICT.I.06-79.CS.E.V2.0 Workstations, Mobile Devices and BYOD Security Standards
- DICT.I.06-80.CS.E.V2.0 Proxy Security Standards
- DICT.I.06-81.CS.E.V2.0 Key Management Standards
- DICT.I.06-82.CS.E.V2.0 Protection against Distributed Denial of Service (DDOS) attacks
- DICT.I.06-83.CS.E.V2.0 Data Diode Standards
- DICT.I.04-34.CS.E.V2.0 Change Management Procedures
- DICT.I.04-35.CS.E.V2.0 Backup and Restoration Procedures
- DICT.I.04-36.CS.E.V2.0 System Acquisition, Development and Maintenance Procedures
- DICT.I.04-37.CS.E.V2.0 Anti-Malware Procedures
- DICT.I.04-38.CS.E.V2.0 Cybersecurity Audit Procedures
- DICT.I.04-39.CS.E.V2.0 Vulnerabilities Assessment Procedures
- DICT.I.04-41.CS.E.V2.0 Cybersecurity Documents Development Procedures

18 References

Department Name	National Institute of Standards and Technology (NIST)	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts for Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Basic Cybersecurity Controls
Access Control Policy	AC-1, MP-1	A.9.1.1	2-2	2-2	2-2	2-2	2-2
Information Classification Policy	RA-2, AC-3, AC-4, AC-16, MP-2, MP-3, SC-16	A.8.2	-	5-2	6-2	6-2	7-2
Internal Threat Mitigation Policy	PM-12	A.12.2.1	-	-	-	-	-
Operational Security Policy	SC-38	A.12.1	-	-	-	-	-
Acceptable Use Policy for Assets	AC-20, PL-4, PS-6	A.8.1.3	-	-	-	-	1-2
Vendor and Third-Party Security Policy	PL-8, SA-12	A.15.1.1	1-4	1-3	-	1-4	1-4
Incident Management Policy	AU-6, IR-1, IR-6	A.16	-	7-2	12-2	-	13-2
Asset Management Policy	PM-5, CM-8, CM-9	A.8	1-2	1-2	1-2	1-2	1-2
Bring Your Own Device (BYOD) Policy)	AC-19	A.6.2.1	5-2	4-2	5-2	5-2	6-2
Password Security Policy	IA-5	A.9.2.3	-	2-2	2-2	2-2	2-2
Clean Desk and Clear Screen Policy	AC-1, AC-11, MP-1, MP-2, MP-4	A.11.2.9	-	-	-	-	-
Change Management Policy	CM-2, CM-3, CM-4, CM-5, CM-9, SA-10	A.12.1.2	-	-	-	3-1	6-1
Backup Policy	CP-9	A.12.3.1	-	-	8-2	8-2	9-2
Human Resources Security Policy	XX-1 controls, PL-4, PS-2, PS-6, PS-7	A.7	4-1	3-1	3-1	5-1	9-1

Encryption Policy	SC-12, SC-13	A.10.1.1	7-2 15-2	-	7-2	7-2	8-2
Physical and Environmental Security Policy	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.9.1.4, A.9.1.5, A.10.1.1, A.15.1.1, A.15.2.1	A.11	-	-	-	-	14-2
System Ownership, Development, and Maintenance Policy	SA-1, SA-4	A.14	-	-	-	3-1 13-2	6-1
Malware Protection Policy	SI-3	A.12.2.1	-	3-2	-	3-2	3-2
Network Security Policy	AC-3, AC-17, AC-18, AC-20, CA-3, SC-5, SC-7, SC-8, SC-10	A.13.1	-	-	4-2	4-2	5-2
Business Continuity and Cybersecurity Policy	CP-1, CP-2, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13	A.17.1	1-3	-	-	1-3	1-3
Cybersecurity Compliance Policy	XX-1 controls, CA-2, CA-7	A.18	-	-	-	-	-
Email Policy	AC-3, PT-4, DS-2	A.13.2.1, A.13.2.3	-	-	-	-	4-2
Cloud Computing Security Policy	AC-20	A.13.1.2	-	1-3	1-3	2-4	2-4
Security Information and Event Management (SIEM) Policy	PT-1, AE-2, AE-3, CM-3, CM-7,	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4	11-2	6-2	11-2	11-2	12-2
Patch Management and Remediation Policy	RA-5	A.12.6.1, A.8.2.1	-	3-2	3-2	3-2	3-2
Web Application Protection Policy	-	A.14.1.2, A.14.1.3, A.14.2.8	-	-	-	12-2	15-2
Vulnerability Management and Penetration Testing Policy	IP-12, CM-8, MI-3, RA-1	A.12.6.1	9-2	-	9-2	9-2 10-2	10-2 11-2

Data Protection Policy	-	-	6-2	5-2	6-2	6-2	7-2
Cookie Policy	-	-	-	-	-	-	-
Remote Work Policy	-	A.6.2.2	-	-	4-2	-	-
Operations Security Policy	-	-	-	-	-	-	-
Data Sharing Policy	-	-	-	-	-	-	-
Data Management Policy	-	-	-	-	-	-	-
Data Storage Policy	-	-	-	-	-	-	-
Cybersecurity Policy for Protecting rinters and Scanners with Photocopiers	-	-	-	-	-	-	-

--------------------------------------End of Document---------------------------------------