GRC REPORT

CYBERBULWORK

YEAR OF REPORT 2025

Table of Contents

List of Figures

Executive Summary

Cyberbulwork has developed a comprehensive information security policy framework that complies with ISO 27002:2022 requirements to safeguard organizational assets against increasing cyber threats. The framework comprises ten essential policies that address critical security areas such as access control, incident management, data protection, and third-party security. The structure, led by a dedicated security team of nine specialists with defined responsibilities, reflects Cyberbulwork's commitment to ensuring the confidentiality, integrity, and availability of corporate and client data.

Each policy is meticulously organized, with specified ownership, authorship, review, and approval processes to ensure accountability. The policies are aligned with specific ISO 27002:2022 domains and provide comprehensive guidelines for all aspects of information security, including password protection, privileged account management, disaster recovery, and clear desk policies. Cyberbulwork has also established a robust compliance framework and utilized the Wizer platform to communicate and monitor policy implementation across the organization.

To enhance the effectiveness of this security framework in a constantly evolving threat landscape, recommendations include increasing security awareness training, implementing Zero Trust principles, automating threat response, bolstering third-party security oversight, and instituting regular policy review processes. These strategies will assist Cyberbulwork in remaining resilient to the rising threat landscape. Cyber threats while also guaranteeing regulatory compliance and stakeholder confidence.

1.0 Introduction

Organizations face increasingly complex cyber-attacks in today's digital world, making information security a vital business responsibility. Cyberbulwork acknowledges this challenge and has developed a comprehensive information security policy framework following ISO 27002:2022 requirements to protect its digital assets and maintain customer trust.

This report thoroughly examines Cyberbulwork's information security policy framework, which comprises ten core policies that address significant security concerns. The security framework is overseen by a nine-member security team with specialized roles covering privileged account management, IT security, cybersecurity engineering, system administration, data governance, risk compliance, and security operations.

The report outlines each policy's ownership structure, ISO compliance mapping, detailed guidance, and implementation framework. It explains how these policies were communicated to employees using the Wizer platform and offers recommendations to ensure the security framework's successful adoption and ongoing effectiveness.

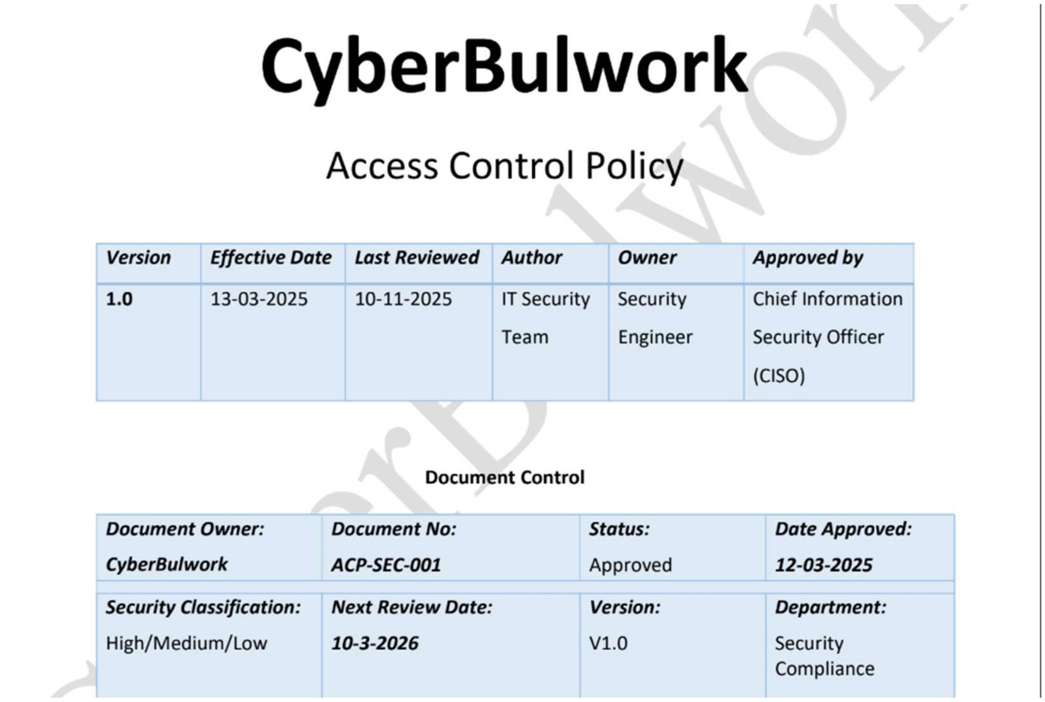
By establishing this robust security foundation, Cyberbulwork demonstrates its commitment to protecting sensitive information assets, fulfilling regulatory obligations, and sustaining a strong security posture amidst emerging cyber threats. The following sections will explore each framework component in detail, illustrating the interconnections between policies and how they collectively contribute to Cyberbulwork's overall security strategy.

1.1 Role Assignment

ROLE	**NAME**
Privileged Account Management Manager	Etinosa Imafidon
IT Security Manager	Ololade Adesagaba
Cybersecurity Engineer	Motunrayo Sanusi
System Administrator	Oluwaseyi Adebayo
Data Governance Manager	Dike Promise

Risk & Compliance Manager	Daniel Owoeye-wise
IT Security EngineerN	Luqman Alli-Balogun
IT Security Engineer	Shado Peculiar
SOC Analyst	Muizz Majeed

2.0 Representation of Policies, Owners, Authors, Reviewers, and Approvers.



CyberBulwork

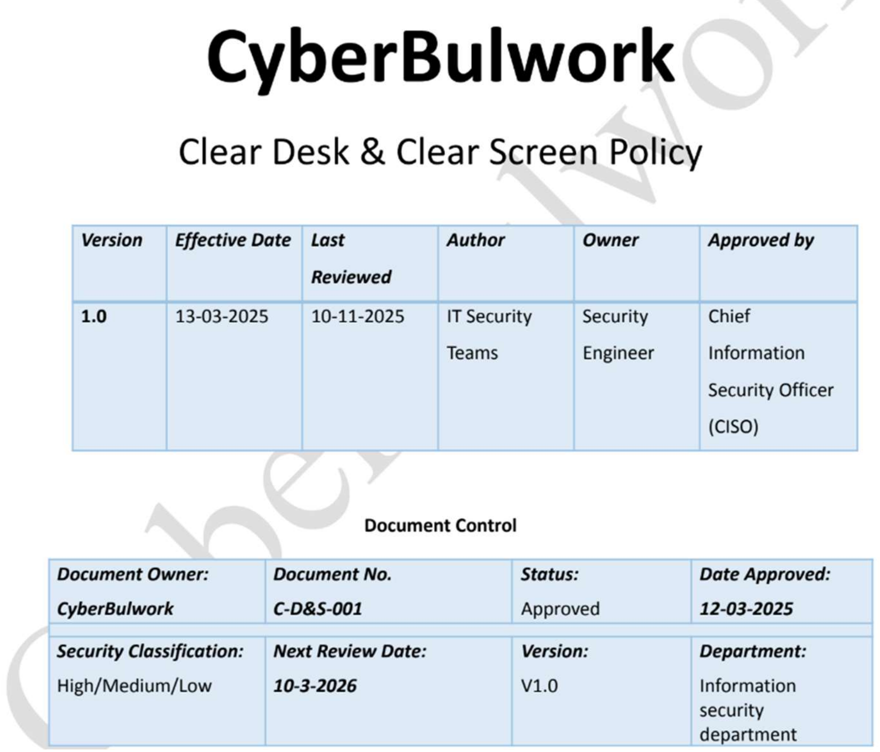
Access Control Policy

Version	*Effective Date*	*Last Reviewed*	*Author*	*Owner*	*Approved by*
1.0	13-03-2025	10-11-2025	IT Security Team	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No:*** ***ACP-SEC-001***	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***10-3-2026***	***Version:*** V1.0	***Department:*** Security Compliance

Figure 1: Access Control Policy



CyberBulwork

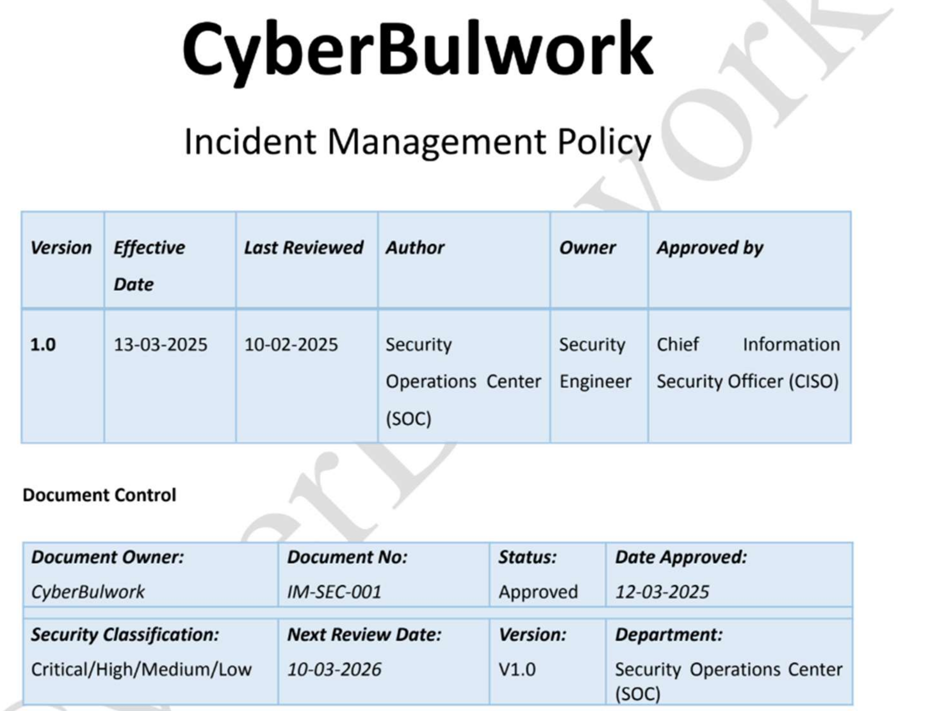
Clear Desk & Clear Screen Policy

Version	*Effective Date*	*Last Reviewed*	*Author*	*Owner*	*Approved by*
1.0	13-03-2025	10-11-2025	IT Security Teams	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No.*** ***C-D&S-001***	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***10-3-2026***	***Version:*** V1.0	***Department:*** Information security department

Figure 2: Clear Desk and Clear Screen Policy



CyberBulwork

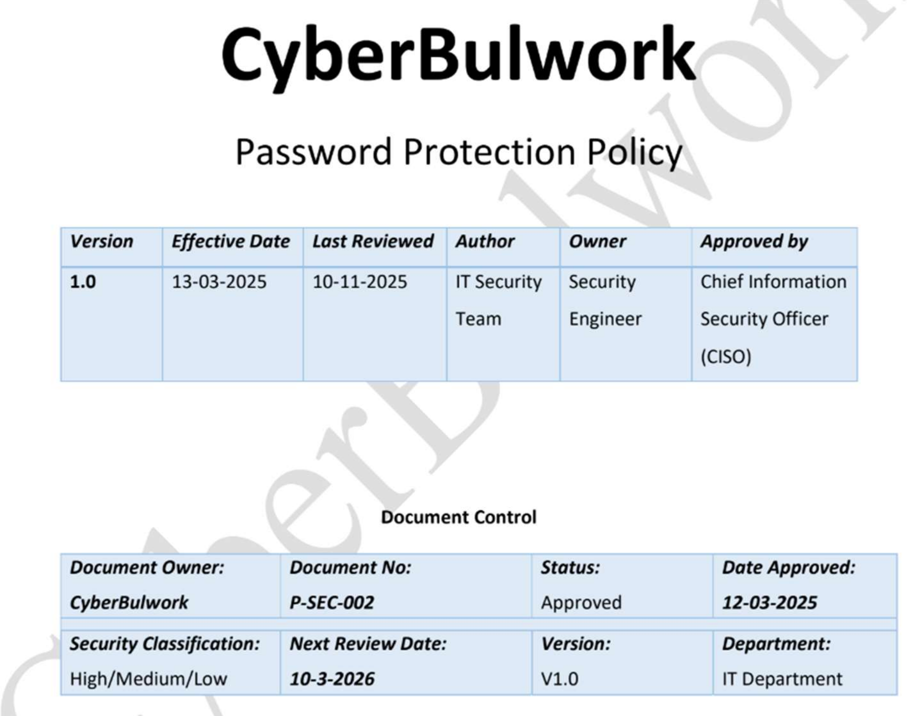
Incident Management Policy

Version	Effective Date	Last Reviewed	Author	Owner	Approved by
1.0	13-03-2025	10-02-2025	Security Operations Center (SOC)	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: *CyberBulwork*	***Document No:*** *IM-SEC-001*	***Status:*** Approved	***Date Approved:*** *12-03-2025*
Security Classification: Critical/High/Medium/Low	***Next Review Date:*** *10-03-2026*	***Version:*** V1.0	***Department:*** Security Operations Center (SOC)

Figure 3: Incident Management Policy



CyberBulwork

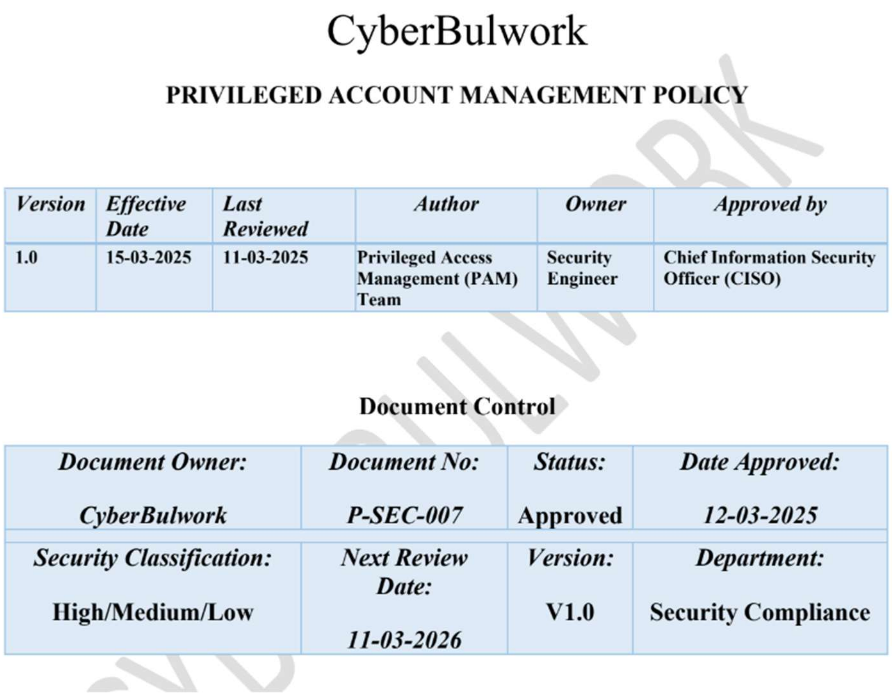
Password Protection Policy

Version	Effective Date	Last Reviewed	Author	Owner	Approved by
1.0	13-03-2025	10-11-2025	IT Security Team	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No:*** ***P-SEC-002***	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***10-3-2026***	***Version:*** V1.0	***Department:*** IT Department

Figure 4: Password Protection Policy



CyberBulwork

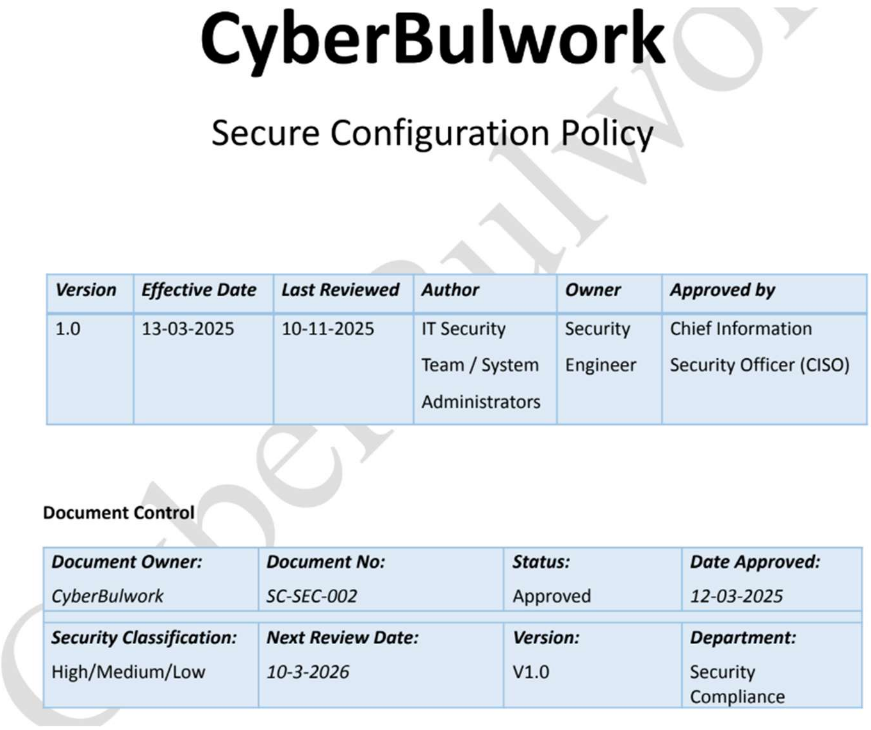
PRIVILEGED ACCOUNT MANAGEMENT POLICY

Version	*Effective Date*	*Last Reviewed*	*Author*	*Owner*	*Approved by*
1.0	15-03-2025	11-03-2025	Privileged Access Management (PAM) Team	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: *CyberBulwork*	*Document No:* *P-SEC-007*	*Status:* Approved	*Date Approved:* *12-03-2025*
Security Classification: High/Medium/Low	*Next Review Date:* *11-03-2026*	*Version:* V1.0	*Department:* Security Compliance

Figure 5: Privileged Account Management Policy



CyberBulwork

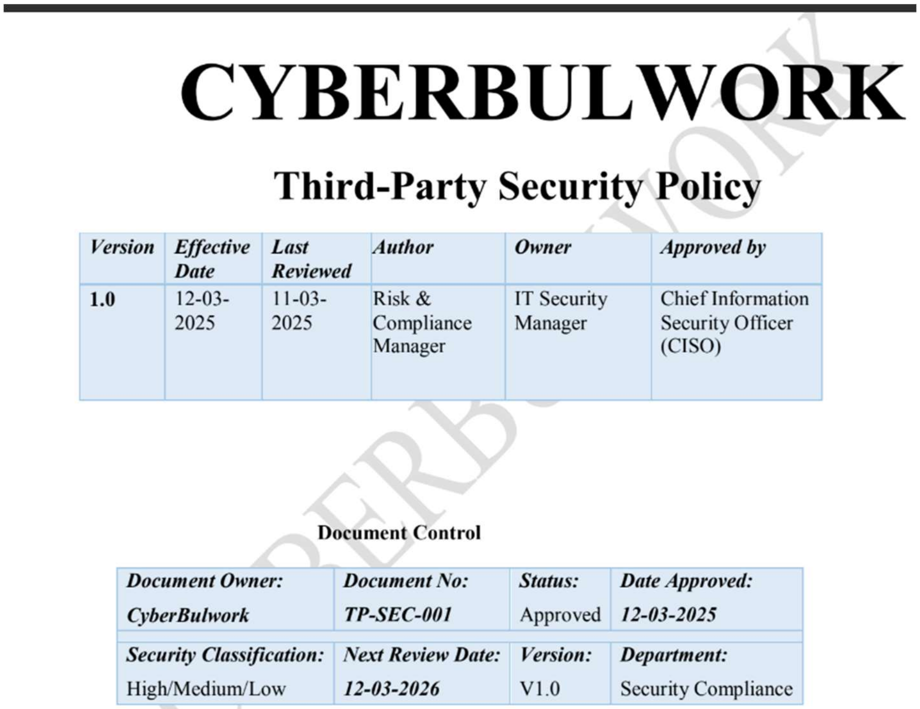
Secure Configuration Policy

Version	*Effective Date*	*Last Reviewed*	*Author*	*Owner*	*Approved by*
1.0	13-03-2025	10-11-2025	IT Security Team / System Administrators	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: *CyberBulwork*	*Document No:* *SC-SEC-002*	*Status:* Approved	*Date Approved:* *12-03-2025*
Security Classification: High/Medium/Low	*Next Review Date:* *10-3-2026*	*Version:* V1.0	*Department:* Security Compliance

Figure 6: Secure Configuration Policy



CYBERBULWORK

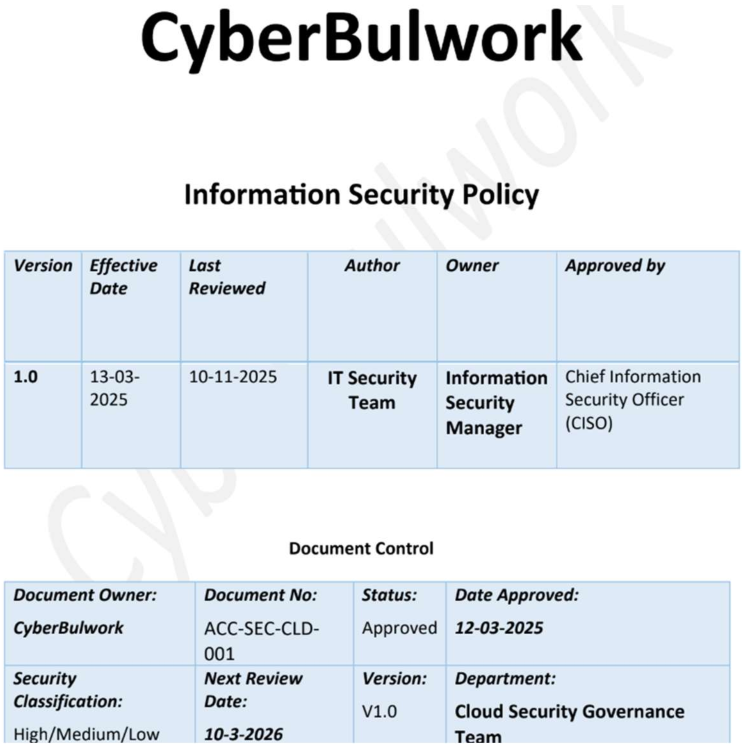
Third-Party Security Policy

Version	*Effective Date*	*Last Reviewed*	*Author*	*Owner*	*Approved by*
1.0	12-03-2025	11-03-2025	Risk & Compliance Manager	IT Security Manager	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No:*** ***TP-SEC-001***	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***12-03-2026***	***Version:*** V1.0	***Department:*** Security Compliance

Figure 7: Third-Party Security Policy



CyberBulwork

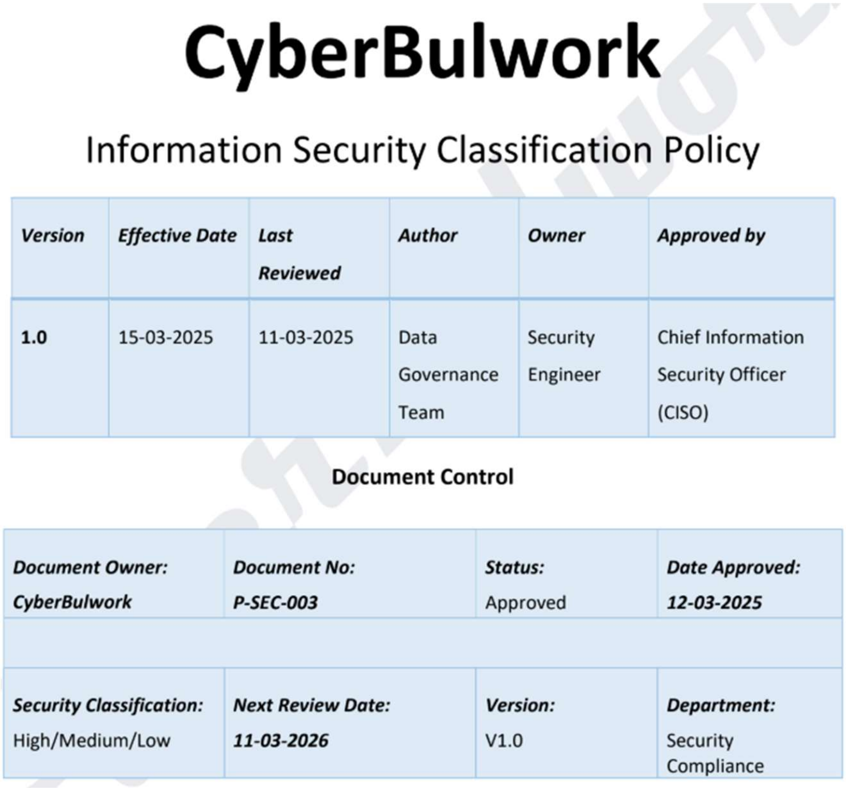
Information Security Policy

Version	*Effective Date*	*Last Reviewed*	*Author*	*Owner*	*Approved by*
1.0	13-03-2025	10-11-2025	**IT Security Team**	**Information Security Manager**	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No:*** ACC-SEC-CLD-001	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***10-3-2026***	***Version:*** V1.0	***Department:*** **Cloud Security Governance Team**

Figure 8: Information Security Policy



CyberBulwork

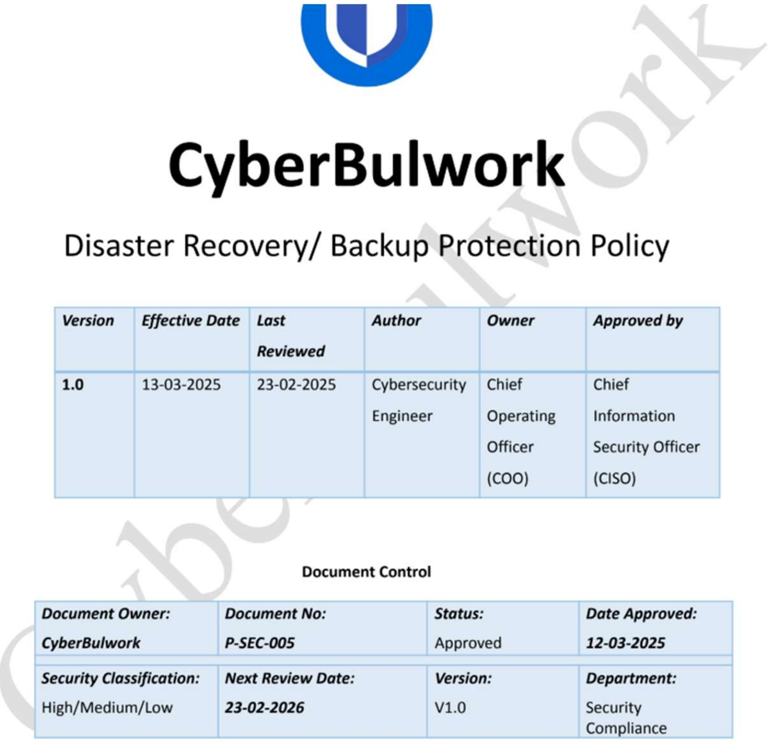
Information Security Classification Policy

Version	Effective Date	Last Reviewed	Author	Owner	Approved by
1.0	15-03-2025	11-03-2025	Data Governance Team	Security Engineer	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No:*** ***P-SEC-003***	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***11-03-2026***	***Version:*** V1.0	***Department:*** Security Compliance

Figure 9: Information Classification Policy



CyberBulwork

Disaster Recovery/ Backup Protection Policy

Version	Effective Date	Last Reviewed	Author	Owner	Approved by
1.0	13-03-2025	23-02-2025	Cybersecurity Engineer	Chief Operating Officer (COO)	Chief Information Security Officer (CISO)

Document Control

Document Owner: ***CyberBulwork***	***Document No:*** ***P-SEC-005***	***Status:*** Approved	***Date Approved:*** ***12-03-2025***
Security Classification: High/Medium/Low	***Next Review Date:*** ***23-02-2026***	***Version:*** V1.0	***Department:*** Security Compliance

Figure 10: Disaster Recovery/Backup Protection

3.0 Domains and sub-domain for each policy

3.1 Password Protection Policy

- ISO 27002:2022: Clause 5.17 - Authentication Information and 5.18 - Privileged Access Rights.
- ISO 27001:2022 Annex A.5.17 (Password Management).

3.2 Access Control Policy

- ISO 27001:2022 Annex A.5 (Access Control).

3.3 Clear Desk and Clear Screen Policy

- ISO/IEC 27002:2022 Annex A.7.7.7.
  Annex A.7.7.10
  Annex A.7.7.1
- ISO/IEC 27002:2022 Annex A.6.6.7.

3.4 Disaster Recovery/ Backup Protection Policy

- ISO 27001:2022 Annex A.5.29

3.5 Incident Management Policy

- ISO 27001:2022 Annex A.5.23 (Event Reporting) and A.5.24 (Incident Response & Recovery)

3.6 Information Security Classification Policy

- ISO 27002:2022(Clause 5.12, 8.2)

3.7 Information Security Policy

- ISO 27002: 5.23 – Information Security for Cloud Services
- ISO 27002: 8.2 – Privileged Access Rights, 8.4 –Access to Source Code

- ISO 27002: 8.1 – User Endpoint Devices, 8.12 – Data Leakage Prevention
- ISO 27002: 8.16 – Monitoring Activities
- ISO 27002: 8.21 – Security of Network Services

3.8 Privileged Account Management Policy

- ISO 27001:2022: Annex A.5.17, A.5.18, A.8.5, A.8.16, A.5.15

3.9 Secure Configuration Policy

- ISO 27002:2022 Annex 8.9

3.10 Third-Party Security Policy

- ISO 27002:2022: A.5.19 Information security in supplier relationships
- ISO 27002:2022: A.5.20 Addressing information security within supplier agreements
- ISO 27002:2022: A.5.21 Managing information security in the ICT supply chain
- ISO 27002:2022: A.5.22 Monitoring, review, and change management of supplier services
- ISO 27002:2022: A.5.23 Information security for the use of cloud services
- ISO 27002:2022: A.5.14 Information transfer

4.0 Policy Statements/Guidelines for Each of the Policies

4.1 Privileged Account Management Policy

1. **Privileged Account Inventory & Classification (ISO 27002: A.5.9, A.5.15, A.5.16)**

   - A centralized privileged account register must be maintained, listing all privileged accounts, their owners, and access levels.
   - Privileged accounts must be categorized based on importance and access scope.

2. **Least Privilege and Access Control (ISO 27002: A.5.15, A.5.18)**

   - Privileged access should be role-based (RBAC) and granted only to individuals who require it for their job functions.
   - Multi-factor authentication (MFA) is mandatory for all privileged accounts.
   - Just-in-time (JIT) access and temporary privilege elevation must be implemented using Azure Privileged Identity Management (PIM).

3. **Secure Authentication & Password Management (ISO 27002: A.5.17, A.8.5)**

   - Privileged account passwords must be stored securely using Azure Key Vault.
   - Passwords must be rotated every 90 days and follow the NIST password guidelines.
   - Privileged accounts must not use shared credentials.

4.2 Secure Configuration Policy

1. **Baseline Standards**:

   - Follow CIS Benchmarks and NIST SP 800-123 for all systems.
   - Cloud environments must adhere to Cyberbulwark’s Cloud Security Framework.

2. **Change Management**:

   - All configuration changes require approval via ServiceNow ticketing.

3. **Vulnerability Mitigation**:
    - Disable unnecessary services (e.g., FTP, Telnet).
    - Encrypt data in transit/at rest (TLS 1.2+, AES-256)

4.3 Third-Party Security Policy

1. **Information Security in Supplier Relationships**
    - Supplier selection processes must consider the risks associated with a supplier's access to Cyberbulwork's information assets.
    - All supplier agreements must include security standards, such as data protection security measures and incident management protocols.
    - Supplier performance must be checked regularly to guarantee continuous compliance.
2. **Ensuring Information Security in Supplier Agreements**
    - Supplier contracts must have terms addressing the following:
    - Data protection and privacy requirements.
    - Incident management and breach notification.
    - Monitoring, auditing, and compliance needs.
    - Contracts must explicitly outline roles, duties, and accountability for security measures.
3. **Maintaining Information Security in the ICT Supply Chain**
    - Implement security measures to address threats across the whole ICT supply chain, including:
    - Conduct background investigations and security assessments on suppliers to verify their security policies and certifications.

- Manage supplier access by using multi-factor authentication (MFA) and role-based access control (RBAC).
- Educate internal teams and suppliers on supply chain risks and security best practices.
- Ensure secure data wipe and access revocation during supplier offboarding.

4.4 Information Security Policy

1. **Cloud Security Governance (ISO 27002: 5.23 – Information Security for Cloud Services)**
   - Establish a cloud security governance framework with defined roles and responsibilities.
   - Conduct regular risk assessments for cloud service providers (CSPs) and ensure compliance with industry standards.
   - Maintain a vendor risk management process for assessing CSP security posture.

2. **Identity & Access Management (ISO 27002: 8.2 – Privileged Access Rights, 8.4 – Access to Source Code)**
   - Implement Zero Trust principles for cloud access control.
   - Enforce multi-factor authentication (MFA) for all privileged and remote access.
   - Restrict and monitor administrative and privileged access rights to cloud-based assets.
3. **Data Protection & Encryption (ISO 27002: 8.1 – User Endpoint Devices, 8.12 – Data Leakage Prevention)**
   - Classify and protect sensitive data using encryption at rest and in transit (AES-256, TLS 1.2/1.3).
   - Implement Data Loss Prevention (DLP) mechanisms for cloud storage, email, and SaaS applications.

- Conduct regular security audits on cloud-hosted data and enforce least privilege access.

4.5 Password Protection Policy

1. **Password Requirements**
   - Minimum Length: 14 characters
   - Complexity: Must include uppercase letters, lowercase letters, numbers, and special characters
   - Expiration: Passwords must be changed every 45 days
   - Reuse Restriction: Users cannot reuse their last 5 passwords
   - Storage: All passwords must be hashed and salted before storage
   - Multi-factor authentication (MFA): Required for all privileged accounts
   - Password Managers: The Usage of company-approved password managers is encouraged
2. **Password Usage Guidelines**
   - Users must never share passwords
   - Cloud access passwords must not be stored in plaintext
   - Passwords must not be written down or saved in unapproved applications
   - Administrative access should be granted only based on business needs

3. **Password Enforcement and Audits**
   - Automated password policy enforcement will be implemented through IAM controls
   - The Security Engineer will conduct regular audits to ensure compliance
   - Any non-compliance will result in a query and possible disciplinary action

4.6 Information Security Classification Policy

1. **Data Transmission and Storage**

- Confidential and Restricted information must be encrypted in transit and at rest.
- Removable media and external storage must be approved for use and encrypted where necessary.
- Information shared with third parties must be protected through contractual agreements and security assessments.

2. **Information Disposal**

- Public and Internal Use Only data may be disposed of through standard deletion methods.
- Confidential and Restricted information must be permanently erased using secure deletion methods or physically destroyed.

3. **Classification Responsibilities**

- **Information Owners**: Responsible for assigning classification levels to information assets.
- **Data Custodians**: Responsible for implementing and maintaining appropriate security controls based on classification levels.
- **Employees and Users**: Responsible for handling information according to its classification and complying with security policies.

4.7 Incident Management Policy

1. **Incident Identification & Reporting:** Employees must report incidents immediately via the IT Help Desk, Cybersecurity Hotline, or Incident Reporting Portal, detailing the nature, impact, and risks.
2. **Classification & Prioritization**: Incidents are categorized by severity (Critical, High, Medium, Low) to determine response urgency and resource allocation.
3. **Response & Resolution**: The Incident Response Team (IRT) follows a structured process: containment, investigation, resolution, and communication.

4. **Documentation & Reporting**: All incidents must be logged in the Incident Management System (IMS) for tracking and analysis.
5. **Post-Incident Review**: Critical and High incidents undergo review to improve policies, procedures, and training.

4.8 Disaster Recovery/ Backup Protection Policy

1. **Disaster Recovery Plan**

   - Recovery Time Objective (RTO): Critical systems must be restored within 4 hours.
   - Recovery Point Objective (RPO): Data loss must not exceed 1 hour of transactions.
   - Failover Procedures: Cloud-based failover mechanisms must be in place for mission-critical applications.
   - Emergency Communication: Employees will be notified via designated communication channels.
   - Roles & Responsibilities: A Disaster Recovery Team (DRT) will oversee recovery procedures.

2. **Disaster Recovery Testing & Audits**

   - Testing Frequency: Disaster recovery simulations must be conducted semi-annually.
   - Audit Compliance: The Security Compliance Team will review disaster recovery logs and adherence to this policy.
   - Incident Reports: Any disaster recovery activation must be documented, analyzed, and reviewed.

3. **Incident Response & Escalation**

   In the event of a disaster:

   - Incident Identification: IT personnel must assess and categorize the incident.
   - Containment & Mitigation: Immediate steps must be taken to prevent further damage.
   - System Recovery: Backup restoration procedures must be initiated.

- Post-Incident Review: A root cause analysis will be conducted to enhance future preparedness.

4.9 Clear Desk & Clear Screen Policy

1. **Clear Desk Guidelines**
   - Secure Storage: Store physical documents containing sensitive information in a locked drawer or cabinet when not in use.
   - Digital Preference: Utilize digital documents over printed copies to minimize physical data.
   - Document Disposal: Shred or securely dispose of sensitive documents; avoid discarding them in the general trash bin. ***Annex A.7.7.10***
   - Device Security: Keep laptops and mobile devices secure when not in use to prevent unauthorized access.
2. **Clear Screen Guidelines**
   - Screen Locking: Lock your computer screen when unattended.
   - Password Protection: Ensure that screensavers and wake-from-sleep modes require password entry.
   - Automatic Lock: Set devices to lock automatically after a period of 5 minutes of inactivity.

4.10 Access Control Policy

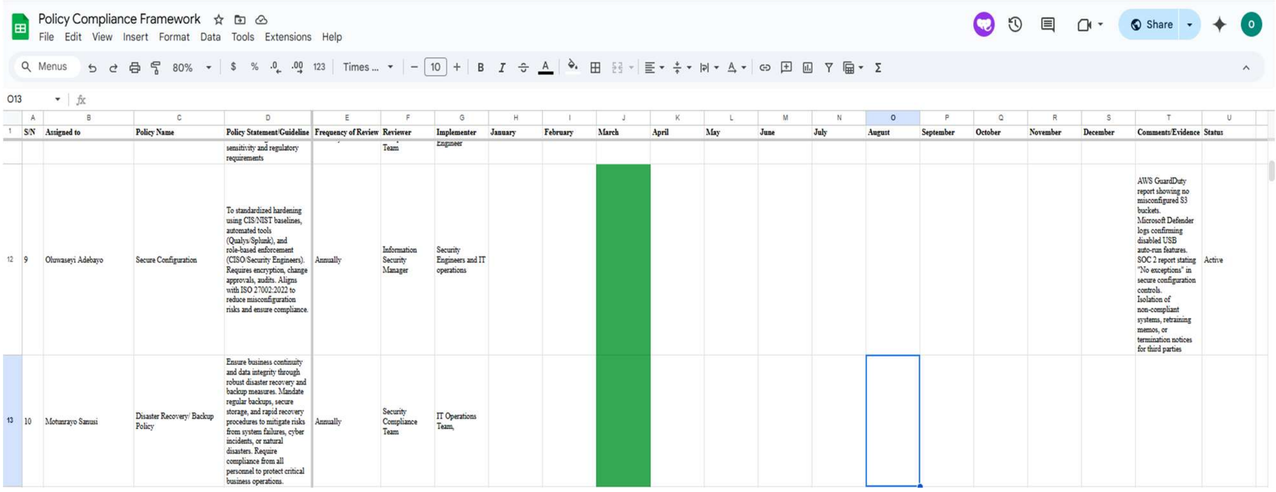
1. **Access Control Principles**
   - Least Privilege: Users are granted the minimum access required to perform their job
   - functions.
   - Role-Based Access Control (RBAC): Access permissions are assigned based on job roles.
   - Separation of Duties: Critical tasks are divided among multiple individuals to reduce
   - risk.
   - Multi-Factor Authentication (MFA): Required for all privileged and sensitive system

- access.
- Access Reviews: Regular audits to verify appropriate access rights.

2. **User Account Management**
   - Onboarding & Offboarding: User accounts must be provided and revoked following a
   - standardized process.
   - Access Requests: All access requests must be approved by the Security Engineer and
   - documented.
   - Temporary Access: Time-limited access must be assigned for specific tasks and removed
   - upon task completion.
   - Password Security: All accounts must adhere to the Password Protection Policy.

5.0 Policy Compliance Framework

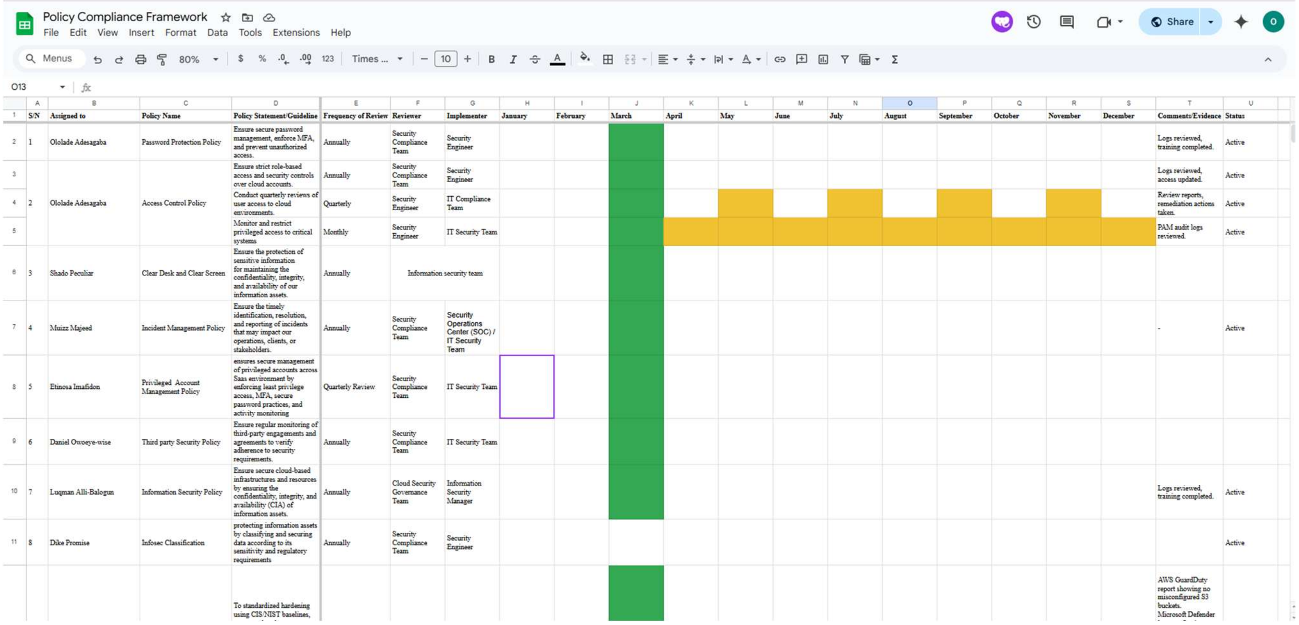
Below is the Policy Compliance Framework for Cyberbulwork



Policy Compliance Framework
File Edit View Insert Format Data Tools Extensions Help
Menus 80% Times ... 10
Share
O13

S/N	Assigned to	Policy Name	Policy Statement/Guideline	Frequency of Review	Reviewer	Implementer	January	February	March	April	May	June	July	August	September	October	November	December	Comments/Evidence	Status
			sensitivity and regulatory requirements		Team	Engineer														
9	Oluwaseyi Adebayo	Secure Configuration	To standardized hardening using CIS/NIST baselines, automated tools (Qualys/Splunk), and role-based enforcement (CISO/Security Engineers). Requires encryption, change approvals, audits. Aligns with ISO 27002:2022 to reduce misconfiguration risks and ensure compliance.	Annually	Information Security Manager	Security Engineers and IT operations			🟩										AWS GuardDuty report showing no misconfigured S3 buckets. Microsoft Defender logs confirming disabled USB auto-run features. SOC 2 report stating "No exceptions" in secure configuration controls. Isolation of non-compliant systems, retraining memos, or termination notices for third parties	Active
10	Motunrayo Sanusi	Disaster Recovery/ Backup Policy	Ensure business continuity and data integrity through robust disaster recovery and backup measures. Mandate regular backups, secure storage, and rapid recovery procedures to mitigate risks from system failures, cyber incidents, or natural disasters. Require compliance from all personnel to protect critical business operations.	Annually	Security Compliance Team	IT Operations Team,			🟩											

Figure 11: Policy Compliance Framework



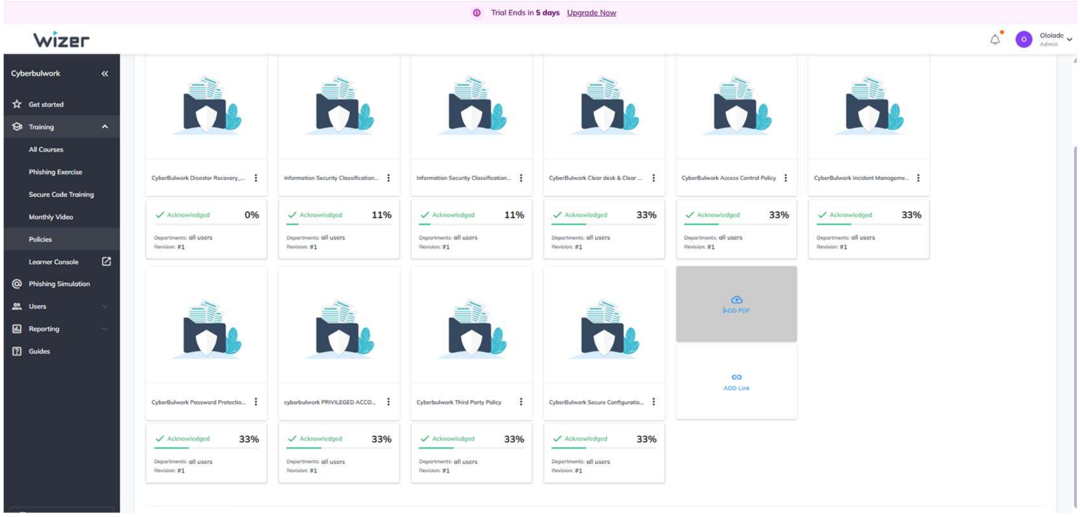
Policy Compliance Framework
File Edit View Insert Format Data Tools Extensions Help
Menus 80% Times ... 10
Share
O13

S/N	Assigned to	Policy Name	Policy Statement/Guideline	Frequency of Review	Reviewer	Implementer	January	February	March	April	May	June	July	August	September	October	November	December	Comments/Evidence	Status
1	Ololade Adesagaba	Password Protection Policy	Ensure secure password management, enforce MFA, and prevent unauthorized access.	Annually	Security Compliance Team	Security Engineer			🟩										Logs reviewed, training completed.	Active
2	Ololade Adesagaba	Access Control Policy	Ensure strict role-based access and security controls over cloud accounts.	Annually	Security Compliance Team	Security Engineer			🟩										Logs reviewed, access updated.	Active
			Conduct quarterly reviews of user access to cloud environments.	Quarterly	Security Engineer	IT Compliance Team			🟩		🟨		🟨		🟨		🟨		Review reports, remediation actions taken.	Active
			Monitor and restrict privileged access to critical systems	Monthly	Security Engineer	IT Security Team			🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	PAM audit logs reviewed.	Active
3	Shado Peculiar	Clear Desk and Clear Screen	Ensure the protection of sensitive information for maintaining the confidentiality, integrity, and availability of our information assets.	Annually	Information security team				🟩											
4	Muizz Majeed	Incident Management Policy	Ensure the timely identification, resolution, and reporting of incidents that may impact our operations, clients, or stakeholders.	Annually	Security Compliance Team	Security Operations Center (SOC) / IT Security Team			🟩										-	Active
5	Etinosa Imafidon	Privileged Account Management Policy	ensures secure management of privileged accounts across Saas environment by enforcing least privilege access, MFA, secure password practices, and activity monitoring	Quarterly Review	Security Compliance Team	IT Security Team			🟩											
6	Daniel Owoeye-wise	Third party Security Policy	Ensure regular monitoring of third-party engagements and agreements to verify adherence to security requirements.	Annually	Security Compliance Team	IT Security Team			🟩											
7	Luqman Alli-Balogun	Information Security Policy	Ensure secure cloud-based infrastructures and resources by ensuring the confidentiality, integrity, and availability (CIA) of information assets.	Annually	Cloud Security Governance Team	Information Security Manager			🟩										Logs reviewed, training completed.	Active
8	Dike Promise	Infosec Classification	protecting information assets by classifying and securing data according to its sensitivity and regulatory requirements	Annually	Security Compliance Team	Security Engineer														Active
			To standardized hardening using CIS/NIST baselines,						🟩										AWS GuardDuty report showing no misconfigured S3 buckets. Microsoft Defender	

Figure 12: Policy Compliance Framework

6.0 Policies Upload on the Wizer Account

The IT Security Manager organized and uploaded the 10 policies that were created. Following the upload, all staff members received an email notification, urging the implementation of these policies. Employees submitted comments to indicate they received the communication.



CyberBulwork Disaster Recovery_...
✓ Acknowledged 0%
Departments: all users
Revision: #1

Information Security Classification...
✓ Acknowledged 11%
Departments: all users
Revision: #1

Information Security Classification...
✓ Acknowledged 11%
Departments: all users
Revision: #1

CyberBulwork Clear desk & Clear ...
✓ Acknowledged 33%
Departments: all users
Revision: #1

CyberBulwork Access Control Policy
✓ Acknowledged 33%
Departments: all users
Revision: #1

CyberBulwork Incident Manageme...
✓ Acknowledged 33%
Departments: all users
Revision: #1

CyberBulwork Password Protectio...
✓ Acknowledged 33%
Departments: all users
Revision: #1

cyberbulwork PRIVILEGED ACCO...
✓ Acknowledged 33%
Departments: all users
Revision: #1

Cyberbulwork Third Party Policy
✓ Acknowledged 33%
Departments: all users
Revision: #1

CyberBulwork Secure Configuratio...
✓ Acknowledged 33%
Departments: all users
Revision: #1

Figure 13: Policies on Wizer

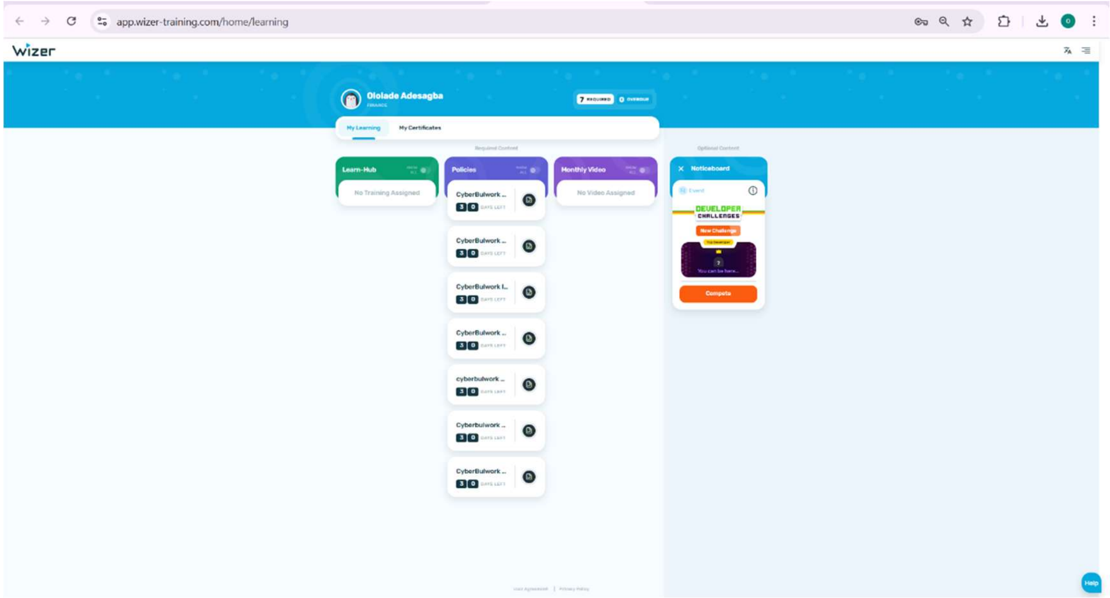


Figure 14: User page showing Policies Access

7.0 Recommendation to Ensure Successful Implementation of the Policy Framework

Cyberbulwork has built a strong foundation for information security by aligning its policies with ISO/IEC 27002:2022, ensuring that critical areas like data protection, access control, and incident response are well covered. Cyberthreats continue to evolve; we must remain one step ahead.

To further strengthen our security posture, we recommend the following:

1. **Make Security Awareness a Daily Habit**
   - Cybersecurity isn’t just an IT concern; it is everyone’s responsibility. By rolling out engaging and interactive security training, including phishing simulations and hands-on exercises, we can empower employees to be our first line of defense.
2. **Adopt a ‘Never Trust, Always Verify’ Approach**

- Implementing Zero Trust principles will ensure that every access request is verified and continuously monitored, whether it's coming from inside or outside our network. This means stricter access controls, risk-based authentication, and continuous monitoring to keep our systems secure.

3. **Respond Faster with Automation**

   - Cyberthreats don’t wait, and neither should we. By automating threat detection and response, we can reduce response times, minimize damage, and free up our security team to focus on more complex threats.

4. **Strengthen Our Third-Party Security**

   - Our security is only as strong as our weakest link, including our vendors. We must ensure all suppliers and third-party partners meet our security standards, undergo regular risk assessments, and have contractual obligations to protect our data.

5. **Keep Our Policies Up to Date**

   - Security policies shouldn’t sit on a shelf collecting dust. We should review and update them regularly, ensuring they evolve with new threats, compliance requirements, and business changes. A dedicated Security Governance Committee can help oversee these updates and drive continuous improvement

8.0 Conclusion

At Cyberbulwork, security isn't just a part of who we are. Our comprehensive security framework reflects our commitment to protecting data, ensuring compliance, and staying ahead of threats. But cybersecurity is a journey, not a destination.

By continuously improving our policies, adopting advanced security practices, and fostering a culture of security awareness, we can ensure that Cyberbulwork remains resilient, compliant, and ahead of emerging threats.

With strong leadership, engaged employees, and the right technology, we’re not just preventing cyber attacks, we’re building a trusted, secure future for our company and customers.