**Cybersecurity Templates**

**Resource Management Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Resource Management Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[1. Purpose 3](#_Toc206701931)

[2. Scope 3](#_Toc206701932)

[3. Policy Framework 3](#_Toc206701933)

[4. Roles and Responsibilities 3](#_Toc206701934)

[5. Resource Management Principles 3](#_Toc206701935)

[5.1 Human Resources 3](#_Toc206701936)

[5.2 Technology and Tools 4](#_Toc206701937)

[5.3 Information Assets and Data 4](#_Toc206701938)

[5.4 Third-Party Resources 4](#_Toc206701939)

[6. Capacity Planning and Allocation 4](#_Toc206701940)

[7. Risk Appetite and Resource Exceptions 4](#_Toc206701941)

[8. Monitoring, Reporting, and KPIs 4](#_Toc206701942)

[9. Budgeting and Procurement Governance 4](#_Toc206701943)

[10. Policy Enforcement 5](#_Toc206701944)

[11. Compliance and References 5](#_Toc206701945)

[12. Review and Maintenance 5](#_Toc206701946)

[13. Appendices 5](#_Toc206701947)

# Purpose

The purpose of this Resource Management Policy is to ensure that adequate human, technological, and financial resources are identified, allocated, and managed effectively to support the organization’s cybersecurity objectives. This policy ensures resilience, efficiency, and compliance with recognized cybersecurity standards and frameworks.

# 2. Scope

This policy applies to all organizational units, employees, contractors, third-party service providers, and stakeholders who are involved in the management, allocation, or use of cybersecurity-related resources.

# 3. Policy Framework

This policy aligns with international cybersecurity standards and frameworks, including ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF), as well as relevant national regulatory requirements. The framework ensures a structured approach to resource governance, risk-based allocation, and continuous improvement.

# 4. Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Chief Information Security Officer (CISO) | Overall accountability for cybersecurity resource allocation and strategy. |
| IT Security Team | Implements and monitors resource use across security domains. |
| Asset Owners | Ensure proper use, reporting, and safeguarding of assigned resources. |
| Procurement Department | Ensures procurement aligns with approved cybersecurity standards and budget. |
| All Employees | Adhere to cybersecurity practices and report deficiencies in resource availability. |

# 5. Resource Management Principles

## 5.1 Human Resources

* Staffing must align with minimum cybersecurity coverage requirements.
* Roles must be defined, trained, and supported by continuous professional development.

## 5.2 Technology and Tools

* Security tools must be evaluated, approved, and maintained with lifecycle management.
* Coverage metrics (e.g., EDR, firewalls, logging) must meet defined thresholds.

## 5.3 Information Assets and Data

* All assets must be inventoried, classified, and tracked in a Resource Register.
* Data protection, backup, and disposal must comply with regulations.

## 5.4 Third-Party Resources

* Third-party providers must meet cybersecurity requirements through contracts and SLAs.
* Vendor performance must be reviewed annually or upon significant changes.

# 6. Capacity Planning and Allocation

The organization must plan and allocate sufficient resources for cybersecurity activities, ensuring critical operations maintain resilience against emerging threats.

# 7. Risk Appetite and Resource Exceptions

Resource gaps beyond acceptable risk thresholds must be escalated for executive approval. Documented exceptions must include risk justification and mitigation steps.

# 8. Monitoring, Reporting, and KPIs

Cybersecurity resource usage will be monitored quarterly and reported to the Security Committee every quarter. KPIs may include staffing fulfillment, log coverage %, backup success rate, and patching SLAs.

# 9. Budgeting and Procurement Governance

Cybersecurity budgeting must be risk-based and reviewed annually. The procurement of security resources must comply with both organizational and legal requirements.

# 10. Policy Enforcement

Failure to comply with this policy may result in disciplinary measures, termination of the vendor contract, or escalation to regulatory authorities, depending on the nature of the violation.

# 11. Compliance and References

This policy supports compliance with ISO/IEC 27001, NIST CSF, and other applicable national or industry-specific regulations.

# 12. Review and Maintenance

This policy will be reviewed annually or following major incidents, organizational changes, or regulatory updates. The CISO is responsible for its upkeep.

# 13. Appendices

* Appendix A: Resource Register (Template)
* Appendix B: Staffing & Competency Matrix
* Appendix C: Supplier & SLA Register
* Appendix D: Annual Resourcing Plan
* Appendix E: Glossary of Terms