Comprehensive Cybersecurity Policy Framework - Structured Overview

This is a complete set of **cybersecurity policy templates** designed to help organizations establish a comprehensive cybersecurity strategy. These policies are interconnected and reference each other to create a cohesive security framework.

Document Structure Summary

The framework consists of **8 core policy documents**:

1. **Cybersecurity Policy (BASIC)** - Master policy document
2. **Access Control Policy**
3. **Asset Management Policy**
4. **Backup and Recovery Policy**
5. **Cyber Incident Response Plan (CIRP)**
6. **Network Security Policy**
7. **Password Policy**
8. **Vulnerability and Patch Management Policy**

1. CYBERSECURITY POLICY (BASIC) - Master Framework

Purpose

Defines minimum cybersecurity requirements for all departments to protect intellectual property, commercial advantage, and personnel from information security consequences and cyber-attacks.

Policy Principles

1. Effective Policies and Procedures

- Awareness of information security risks
- Collaborative creation of security policies
- Clear responsibilities and rule application

2. Environment Knowledge and Risk Management

- Understanding of important information systems
- Risk identification and maintenance at acceptable levels
- Continuous improvement cycle for security adaptation

3. Secure Product/Service Development

- Built, tested, and maintained with cyber-security and privacy considerations

4. Robust Infrastructure

- Designed for high availability of vital systems

5. Proactive Action

- Regular patching
- Vulnerability awareness and monitoring
- Learning from security events and incidents

6. Proper Personal Data Handling

- GDPR compliance ((EU) 2016/679)
- Necessary technical and organizational measures

Scope

Applies to:

- All information and systems
- Information systems provided
- People (internal and external) processing information
- Devices used for processing
- Procedures and dependencies
- Work locations
- Other risk-posing aspects

Critical and confidential information: Information/systems that would harm the organization if confidentiality, integrity, or availability is compromised.

Minimum Requirements

Environment Management:

- Defined and communicated cybersecurity roles and responsibilities
- Inventory of all physical devices, systems, and software
- Proper maintenance of equipment essential to critical systems
- Approved antivirus/anti-spyware/anti-malware programs installed and updated
- Secured corporate network per network security policy
- OS and application patches/security updates per vulnerability management policy

Personnel Awareness:

- Regular awareness training on cyber risks and threats
- Communication of **10 Golden Rules for Cybersecurity**
- Agreement to abide by security rules

Access Management:

- Multi-factor Authentication (MFA)
- Minimum access principle (detailed in Access Policy)
- Strong passwords (detailed in Password Policy)
- Successful login/logoff logging for critical systems

Disaster Recovery:

- Process to recover critical systems
- Process to restore critical documents/records
- Detailed in Backup and Recovery Policy

Incident Response:

- Response plan for cyber incidents

2. ACCESS CONTROL POLICY

Purpose

Determines who has access to data, applications, and digital assets, and under what circumstances. Secures digital environments through authentication and authorization.

Core Principles

Minimum Access Principle:

- Every user (internal/external) receives exactly sufficient access to perform their function
- Standard Multi-factor Authentication (MFA) enforced where possible

Remote Access:

- Restricted to designated users from untrusted locations
- VPN connections for organizational laptops
- Regular access checks and modifications via Account Creation/Modification Form (ACMF) or Account Removal Form (ARF)

Account Management

User Accounts (for critical and confidential systems)

Requirements:

- Unique and personal
- Password protected per Password Policy
- Requested only by authorized persons
- Withdrawn when obsolete (e.g., contract termination)

Privileged Accounts

Rules:

- Restricted assignment (domain administrator, super user, root)
- Used only when privileged access needed
- Owners use non-privileged accounts for normal activities
- Account names should not disclose extended privileges
- MFA required for critical/confidential systems accessed from untrusted networks

Shared Accounts

Controls:

- Use should be prevented if possible
- If unavoidable, controls required for:
    - Knowing who can use the account
    - Controlling account use
    - Password change process and communication
    - Preventing abuse upon contract termination

External Staff and External Company Accounts

Additional Requirements:

- Easily identifiable (prefix or description)
- Revoked at contract end
- If automatic revocation cannot be ensured: automatic expiry every **[3 months]** unless officially renewed

Service Accounts (Machine-to-Machine)

Requirements:

- Easily identified as service account (prefix or description)
- Minimum access principle applies
- Interactive use should be avoided

Authentication and Authorization

Microsoft Active Directory (AD):

- Centralized authentication and authorization solution

- Rights and security settings management across network
- Integrated with Windows environment
- Allows delegated management

Authentication Requirements

- Secure connection procedure for access control
- IT manager records and monitors all connection attempts
- Initial passwords securely transmitted directly to user
- Passwords set to change immediately
- Multi-factor authentication used where appropriate and feasible
- Account suspension after **[3 attempts]** within **[5 minutes]**
- Access suspension when account unused for **[e.g., 90 days]**

Authorization Requirements

- Access requests only via ACMF/ARF form
- Requested only by HR responsible or N+1 of person concerned
- Formal approval by **[organization responsible]** required
- IT responsible grants, updates, and removes access rights
- Authorization groups used; role-based access granting

3. ASSET MANAGEMENT POLICY

Purpose

Establish guidelines for managing assets per ISO 27002, CIS Controls v8, and IEC 62443 standards. Ensures availability, integrity, and confidentiality of all physical and digital assets.

Key Definitions

Term	Definition
Assets	All data, information, and information systems owned/operated by organization (hardware, software, databases, networks, domain names, documentation)
Critical Assets	Resources/components essential to organization's operation and success
IACS Assets	Hardware, software, network components, and information part of industrial automation and control systems
Asset Owner	Designated person/team managing specific information and IACS assets
Media	Physical devices storing data (hard drives, SSDs, USB sticks, CDs/DVDs, tapes, mobile devices)
Sensitive Data	Confidential, personally identifiable, or business-critical information requiring protection

Responsibilities

Asset Owners:

- Maintain accuracy of asset records
- Identify security requirements
- Coordinate maintenance and repair

Staff:

- Proper use and maintenance of assigned assets
- Report issues/incidents per cybersecurity policies

Asset Lifecycle

Key Stages:

1. **Acquisition/Development**
    - New asset acquisition or transfer from another business unit
1. **Discovery/Monitoring/Inventory**
    - Continuous identification of new assets on corporate network
1. **Use**
    - Authorized use by employees, remote suppliers, contractors, service providers, consultants
1. **Controlled Removal**
    - Safe retirement of assets
1. **Uncontrolled Removal**
    - Lost, stolen, or unexplained assets

Inventory Requirements

Primary Assets

Examples:

- Company data, orders, contracts, project data
- Customer data
- Employee personal data
- Specific expertise
- Product/technology data (source code)
- Login credentials
- Confidential information
- Business processes

Required Information:

- Name
- Description
- Owner

- Classification (confidentiality, integrity, availability)
- Personal data records
- Managed by
- Supplier (if applicable)

Secondary Assets (Supporting Assets)

A. (Virtual) Hardware Inventory

Required Information:

- Asset identification code
- Date of purchase/depreciation
- Description
- Manufacturer
- Model number
- Serial number
- Firmware version
- Asset owner name/role/business unit
- Physical location
- Physical (MAC) address
- Warranty expiration date

Important Notes:

- Include virtual assets (external Cloud platforms)
- Record technical specs, support info, customer info, vendor info
- Ensure Cloud hardware meets same requirements
- **Don't forget**: Domain names, private keys for certificates, other crypto items

B. Software Inventory

Required Information:

- Name
- Description
- Owner
- Version
- License information (contract term, number of licenses)
- Supplier contact information
- Contract number
- Optional: Dates SW handles
- Distinction between unsupported and unauthorized software

Review Frequency: [Responsible department] checks inventory **semi-annually or more often**

Use and Maintenance

Use Requirements

- Handle all assets with care
- **[Semi-annual]** or more frequent inspections (in-person or remote) unless exception authorized
- Asset owner responsibilities:
    - Maintain control of asset
    - Contact **[responsible service]** for problems (malfunctions, repairs, underutilized equipment, loss)

Preventive Maintenance

- Regular maintenance and updates on endpoints (laptops, desktops, workstations, servers)
- Per Vulnerability and Patch Management Policy
- Document all maintenance activities (separate logbook or in inventory)

Corrective Maintenance

- Address defects/security incidents immediately
- Document incidents
- Analyze incidents and take corrective actions to prevent recurrence

Security of Assets

Physical Security

- Assets physically secured against unauthorized access, theft, damage
- Measures: access control, locks, secure storage areas

Network Security

- Network segmentation to separate critical IACS components
- Firewalls, Intrusion Detection Systems (IDS), other network security measures
- Per Network Security Policy

Access Management

- Per organization's Access Policy
- Authentication and authorization per Password Policy

Data Protection

- Encrypt sensitive data during transfer and storage
- Regular backups per Backup and Recovery Policy

Safe Removal and Destruction

Controlled Removal

Process:

- Return assets to **[responsible department]**
- Copy user data if necessary
- Securely erase primary memory storage (encryption, shredding per DIN-66399 standard, degausser)
- Remove old documents, policy notes, SOPs, manuals (keep log)
- Update asset status in all enterprise management systems
- Document removal from inventory

Domain Names:

- Delete old domain names or keep them under control during transition period
- Risk of domain hijacking by scammers/cybercriminals
- Old domains may still receive sensitive emails
- Often linked to cloud accounts (Dropbox, OneDrive, iCloud, Google Drive)
- Registration cost minimal compared to potential damage

Resources:

- DNS Belgium: Domain management guidance

Uncontrolled Removal

- Report lost/stolen assets immediately to **[responsible department]**
- Remove from inventory

Incident Management

- Report all security incidents immediately per organization's Cyber Incident Response Plan
- Analyze incidents
- Take corrective actions to prevent recurrence

Training and Awareness

- All employees receive training on asset management and security responsibilities
- Regular awareness campaigns
- **4 training opportunities per year**
- Content includes:
    - 10 Golden Rules of Cybersecurity
    - Lessons learned from cyber incidents
- Additional campaigns as needed

Compliance and Audit

- Regular internal controls for policy compliance
- Compliance with applicable laws and regulations

- Information and IACS security standards

Changes and Deviations

- Changes approved by **[organization]** management
- Variations granted only with written approval of **[Function]**

4. BACKUP AND RECOVERY POLICY

Purpose

Protect critical information and information systems against data loss and damage through backup and recovery procedures.

Note: Backup not necessary when:

- Data loss is acceptable
- Other control measures overcome disaster situations
- Example: PLC system with static configuration easily redeployed/replaced

Responsibilities

- **Owner:** Responsible for efficient backup and recovery process meeting business needs
- **Operational tasks:** Can be delegated to system administrators or vendors

Backup and Recovery Procedure

Required for all critical systems, defining:

- What information to backup (systems AND data)
- How to make backup
- Backup monitoring
- When and how often to backup
- How long to keep backup
- How and where to store backup
- How backup data is transferred

RPO and RTO

RPO (Recovery Point Objective):

- Maximum period during which data can be lost due to major incident
- Example: Static copy made nightly at 2 AM = 24-hour maximum data loss

RTO (Recovery Time Objective):

- Length of time required to recover data

Recommended: Use GFS (Grandfather-Father-Son) scheme (see Annex 1)

Access to Backup and Encryption

Requirements:

- Backups have at least same protection level as original data
- Encrypt confidential backup data when:
    - Physically/logically stored in accessible locations
    - Network traffic for backup
    - Backup media stored/transferred by unauthorized persons
    - Backup files on media in accessible locations
- Backup encryption key for off-site media not stored only on-site

Offsite Backup

- Store backup data in different physical location from data itself
- Maintain overview of off-site media
- **Recommended:** Use 3-2-1 backup strategy (see Annex 2)

Backup Monitoring

- Monitor backup process for proper operation
- Address errors
- Demonstrate proper operation via logs, reports, or automated system

Recovery Test

- Perform recovery tests **at least once a year** for all backup methods used for critical systems
- Operational restore (unplanned) outside scheduled test counts as recovery test

ANNEX 1: GFS Backup Schedule

What is Grandfather-Father-Son Backup?

Popular data backup method combining full and partial copies to different media to:

- Reduce backup time
- Improve storage security

GFS Backup Rotation Principle

Three Planned Steps:

1. **Grandfather (G):** Full backup to particular site, one off-site or multiple sites
2. **Father (F):** Another full backup, more regularly, to faster storage
3. **Son (S):** Incremental backup (or differential) to same storage as "father"

Example GFS Scheme

Daily Backups (Son):

- Four backup media labeled for weekdays (Monday-Thursday)
- Each tape used on labeled day
- 1-week version history: Overwrite weekly
- 3-week version history (recommended): More tapes needed

Weekly Backups (Father):

- Up to five weekly backup media ("Week1", "Week2", etc.)
- Full backups recorded weekly on day "Son" media not used (Friday)
- Reused monthly
- Five weekly tapes for 1-month file history

Monthly Backups (Grandfather):

- Three media labeled ("Month1", "Month2", etc.)
- Full backups on last business day of each month
- Overwritten quarterly or annually (recommended)

Schematic Representation:

```
Mon Tue Wed Thu Week 1
Mon Tue Wed Thu Week 2
Mon Tue Wed Thu Week 3
Mon Tue Wed Thu Month1
```

Data Backup Techniques

1. Full Backup

- Complete copying of entire data set
- Takes up significant space, time, and resources
- Makes many unnecessary data copies

2. Incremental Data Backup

- After initial full backup, stores only differences from previous incremental backup
- Processes only files that appeared or changed since previous backup

3. Differential Data Backup

- Similar to incremental
- After initial full backup, stores only differences from last full backup

4. Mixed Data Backup

- Combination of full and partial backups (incremental or differential)
- Similar to versioned backup technique
- Full backup followed by fixed amount of partial backups

ANNEX 2: 3-2-1 Backup Strategy

Definition

Proven data protection and recovery method ensuring:

- Data adequately protected
- Up-to-date backup copies available when needed

Basic Concept:

- **3** backups of data to be protected
- **2** different types of storage media
- **1** backup sent to another location

Classic 3-2-1 Scenario

- Backup software backs up mission-critical data
- Backup stored on another on-premises storage device
- Two more backups stored on two other devices
- Traditionally: At least one device was tape library (easy portable backup)
- Modern: Tape often replaced by hard disk storage system

Current Relevance:

- Still embraced by backup vendors as "best practice"
- Valid regardless of how/where company stores data
- Adapted for new requirements and big data

3-2-1 Backup Rules

Rule 1: Three Data Copies

- Three copies of backups of all critical data
- Regular backups (daily or more often)
- Includes original data and at least two backups

Rule 2: Two Types of Storage

- Two different storage types for backup data
- Minimizes risk of failure
- Types: Internal hard drive, external hard drive, removable storage, tape library, secondary storage array, cloud backup

Rule 3: One Off-site Location

- At least one backup copy sent to off-site storage facility
- Ensures natural/geographical disasters cannot affect all copies
- Physically delivered (tape) or replicated via telecommunications

Importance of 3-2-1 Rule

Benefits:

- Eliminates single point of failure for data
- Protects against:
    - Data corruption
    - Technology failures
    - Natural disasters
    - Theft
- Recognized as "best practice" for information security professionals

Data Recovery Process

Step 1: Original (active) data corrupted/damaged/lost

- Restore from backup copy stored internally on another media/secondary storage

Step 2: Second data copy unavailable/unusable

- Retrieve off-site copy to internal servers

Step 3: Restart 3-2-1 process ASAP

- Once suitable data copy attached and operation restored
- Ensure data remains adequately protected

Modern Backup Uses

Development and Testing:

- DevOps requires easy access to data close to live application data
- Backup data provides fresh, regularly generated data

Analytical Applications:

- Need access to large amounts of current data
- Fresh backup data provides reliable, accurate results

Important Considerations:

- If backup copy used for development/analytics: may be modified or unavailable
- Renders one of three required copies unusable if recovery needed

- Manage controls to ensure applications get best possible data

Data Integrity:

- Key concern in data protection
- Not enough to just back up and lock away copies
- Must ensure backups are: complete, undamaged, recoverable
- Recovery testing helps verify integrity
- Advanced backup app features detect ransomware and threats

3-2-1 Backup Management Principles

Basic Principles:

- All data copies identical and up-to-date
- Media storing copies are readable
- All specimens and equipment tested and confirmed working
- Remote copies stored securely
- Recovery regularly tested (single/multiple files or full backup)
- Internal data copies on different storage systems and networks
- Internal copies cannot be accessed from outside company

Backup Software Benefits:

- Automatically controls disposition of backups
- Catalogues all backup activity
- Features to check for threats (malware, ransomware, viruses)

3-2-1 Summary

Best practice combining:

- **GFS scheme:** Focuses on RPO-RTO of data
- **3-2-1 strategy:** Focuses on storing backups made

Example Implementation:

- Data on NAS with RAID 10 disks
- Nightly backup via backup server to separate NAS (separate network)
- Full backup takes >12 hours
- GFS schedule chosen for changing data
- Weekly and monthly backups copied to secure cloud environment
- Combines 3-2-1 strategy with GFS backup schedule

5. CYBER INCIDENT RESPONSE PLAN (CIRP)

Purpose and Objectives

Goal: Support rapid and effective response to cyber incidents aligned with security and business objectives

Objectives:

- Provide guidance on steps needed to respond to cyber incidents
- Outline roles, responsibilities, accountabilities, and authority
- Outline cyber incident compliance requirements
- Outline internal and external communication processes
- Provide guidance on post-incident activities for continuous improvement

Standards and Frameworks

Based on:

- CyberFundamentals Framework (www.cyfun.be)
- NIST SP 800-61 (Computer Security Incident Handling Guide)
- ISO/IEC 27035 series (Information security incident management)
- ISO/IEC 27001 (Information security management systems)
- ISO/IEC 27002 (Information security management measures)
- Australian Cyber Security Center guidelines

Key Definitions and Acronyms

Term	Definition
Significant Incident	Incident significantly affecting service provision causing: serious operational disruption or financial losses; OR affecting others causing significant material/immaterial damage
Near-Incidents	Event that could have compromised availability, authenticity, integrity, or confidentiality but was prevented or did not occur
Cyber Threat	Circumstance/event that can damage systems or information (phishing, ransomware, security weaknesses, supply chain compromise, business email compromise, cybercrime)
Cybersecurity Event	Event indicating possible security policy breach, security failure, or unknown situation relevant to security
Cybersecurity Alert	Notification generated in response to deviation from normal behavior
Cyber Incident	Unwanted/unexpected cybersecurity event with significant probability of compromising business operations; requires corrective action
CEO	Managing Director
CFO	Finance Director
CIO	Chief Information Officer
CIRP	Cyber Incident Response Plan

CIRT	Cyber Incident Response Team
CISO	Chief Information Security Officer
COO	Chief Operating Officer
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DPO	Data Protection Officer
GBA	Data Protection Authority
ICS	Industrial Control System
MT	Management Team
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SPOC	Single Point of Contact

Incident Response Process Flow

Six Main Phases:

1. **Detection, Research, Analysis and Activation**
2. **Incident Classification**
3. **Escalation and De-escalation**
4. **Containment, Evidence Collection and Remediation**
5. **Recovery**
6. **Lessons Learned**

Common Threat Vectors

Type	Description
External/Removable Media	Attack from removable media/peripheral device (malicious code from infected USB)
Failure	Brute force methods to compromise/destroy systems/networks/services (DDoS, brute force authentication attacks)
Web	Attack from website/web-based application (cross-site scripting, malicious redirection)
Email	Attack via email message/attachment (exploit code, malicious links)
Supply Chain Interdiction	Physical implants, Trojans, backdoors by intercepting goods in transit
Imitation	Benign replaced by malicious (spoofing, MITM attacks, rogue access points, SQL injection)
Improper Use	Violation of Acceptable Use Policy (installing file sharing software causing data loss)
Loss or Theft of Equipment	Loss/theft of computing device/medium (laptop, smartphone, verification token)

Common Cyber Incidents and Initial Responses

Type	Initial Response
DoS and DDoS	Follow playbook X and procedures; take local actions; if ineffective, escalate to second line
Phishing	If malicious content identified: warn staff, give copy to security officer, outline next actions and notifications

Ransomware	[Follow specific ransomware playbook]
Malware	[Follow specific malware playbook]
Data Breach	[Follow data breach procedures]
ICS Compromise	[Follow ICS compromise procedures]

Roles and Responsibilities

Contact Points (24/7)

Primary and Secondary (Backup) Contact Points

Name	Opening Hours	Contact Details	Title	Responsibilities
[Primary SPOC]	*9 AM - 6 PM*	*Mobile phone*	*Primary contact for incidents*	*SPOC*

Cyber Incident Response Team (CIRT)

Core CIRT Members:

Name	Organization Role	Contact Details	CIRT Role	Responsibilities
			Cyber Incident Manager	*Scheduling responses, CIRT operations*
			Network Engineers	*Network analysis and remediation*
			System Administrators	*System recovery and security*

Expanded CIRT (Significant Incidents):

Name	Organization Role	Contact Details	CIRT Role	Responsibilities
			Communications Manager	*Information, warnings, internal communication*
			Legal Advisor	*Legal advice, regulatory compliance*

Management Team (MT)

For significant incidents providing strategic oversight:

Focus Areas:

- Identify and manage strategic issues
- Stakeholder engagement and communication
- Resource and capability demands
- Urgent logistical/financial requirements
- Personnel considerations during response

MT Members:

Name	Contact Details	Title	MT Role

CEO	*Chair*
CIO	*Deputy Chairman*
CISO	*Security alert and CIA monitoring*
COO	*Operational functions*
CFO	*Emergency purchases and expenditure monitoring*
Legal Council	*Regulatory compliance, cyber insurance*
Communications Manager	*Public relations and stakeholder engagement*

Communications

Internal Communications

Key Messages for Employees:

- What happened and why?
- What will happen in near future?
- What is expected of employees?
- Who can employees contact with questions?

External Communications

Key Messages for External Stakeholders:

- What happened and why?
- Which systems/services affected?
- Steps being taken to resolve situation
- Estimated resolution timeline
- Expectations from external stakeholders
- Contact information for questions/concerns

Important: All communications reviewed and approved by Communications Manager and Incident Manager before release

NIS2 Reporting Requirements

For Essential and Important Entities (per Belgian NIS2 legislation):

Within 24 Hours of Discovery:

- Is incident result of wrongful or malicious act?
- Does incident have cross-border implications?

Within 72 Hours:

- Update to above information
- Initial assessment (severity and consequences)
- Indicators of degradation

Within 1 Month:

- Final report including:
  - Detailed description (severity and consequences)
  - Threat type or root cause
  - Applied and ongoing risk mitigation measures (technical and organizational)
  - Cross-border impact (if applicable)

If Unresolved After 30 Days:

- Progress report to CERT
- Final report within one month after resolution

Voluntary Reports to CERT:

- Essential/important entities: incidents, cyber threats, near incidents
- Other organizations: significant incidents, cyber threats, near incidents

Supporting Procedures and Scripts

Standard Operating Procedures (SOPs)

- Detection, triage and analysis of events
- Business continuity plan
- Disaster recovery plan

Supporting Playbooks

- Phishing
- Data intrusion/theft
- Malware
- Ransomware
- Denial of Service

Stakeholder Notification and Reporting

Incident Type/Threshold	Organization	Contact Details	Key Requirements	Responsible Staff
Ransomware	Center for Cybersecurity Belgium CERT.BE	info@ccb.belgium.be	https://www.cert.be/en/report-incident-0	Cyber Incident Manager
Personal Data Breach	Data Protection Authority	+32 (0)2 274 48 00	https://www.gegevensbeschermingsautoriteit.be	Legal Counsel or DPO

Additional Requirements:

- List legal and regulatory requirements for business
- Check cyber insurance policy requirements

Incident Response Process Detailed

1. Detection, Research, Analysis and Activation

Incidents Detected Via:

- Self-detected incidents (IDS/IPS systems)
- Notifications from service providers/vendors
- Notifications from trusted third parties (CCB, MITRE ATT&CK, ENISA)

2. Incident Classification

Classification Levels:

Classification	Description
Critical	Critical incident with very high impact; complete system failure, loss of customer data, major security breaches, critical infrastructure failures
High	Major incident with significant impact; partial system failures, critical functionality affected
Medium	Moderate impact; non-critical functionality affected, user inconvenience
Low	Small low-impact incident; non-critical function failures, low-priority user complaints

Classification Factors:

- Consequences (confidentiality, integrity, availability)
- Stakeholders involved (internal and external)
- Type of incident
- Impact on business and community

3. Investigation Questions

- Who discovered or reported incident?
- When was incident discovered or reported?
- Where was incident discovered or located?
- What impact on business operations?
- What is extent within network and applications?

4. Escalation and De-escalation

Roles that can escalate/de-escalate should be documented:

Classification	Action	Reason for Escalation/De-escalation	Decider
Critical	De-escalating to High		
High	Escalating to		

	Critical
High	De-escalating to Medium
Medium	Escalating to High
Medium	De-escalating to Low
Low	Escalating to Medium

5. Containment, Evidence Collection and Remediation

A. Containment

Importance:

- Prevents incident from overwhelming resources
- Reduces damage
- Provides time to develop tailored recovery strategy

Containment Strategies Vary by Incident Type

Criteria for Strategy Selection:

- Possible damage to and theft of resources
- Preservation of evidence
- Availability of services
- Time and resources needed
- Effectiveness of strategy (partial vs. full containment)
- Duration of solution (emergency, temporary, permanent)

Considerations:

- Some attacks cause additional damage when contained
- Example: Malicious process may overwrite/encrypt data when disconnected
- Sandboxing possible but requires legal department discussion
- Delayed containment dangerous (attacker can escalate)

B. Documentation

Information to Document:

- Date and time of incident
- Current status
- Contact details of relevant individuals
- Scope and impact
- Severity
- Type and classification
- Need for external help (with contact information)
- Actions taken to contain and resolve

- Information about next incident update

C. Evidence Collection and Preservation

Evidence Log Requirements:

- Who collected/handled evidence
- Time evidence collected/handled
- Details of each item collected:
  - Physical location
  - Serial number
  - Model number
  - Host name
  - Log files
  - IP address
  - Operating system

Evidence Collection Table:

Date/Time of Collection	Collected By	Evidence Details	Location of Evidence	Access
01/01/2024	*Mr. Janssens*	*Hard drive laptop SN, model no.*	*Disk with SN stored in safe in server room*	*ICT manager, CIRT team*

D. Remediation Action Plan

Questions to Consider:

- What actions needed to resolve incident?
- What resources (internal & external) needed?
- Who owns incident resolution?
- Priority for systems/services?
- On whom and what does resolution affect?
- Timetable for closing incident?

Action Plan Table:

Date/Time	Category	Action	Action Owner	Status
01/01/2024	*Contains*	*Disconnect infected host from network*	*System Administrator*	*In Progress*

6. Recovery

Recovery Plan Development:

Considerations:

- Recovery Time Objective (RTO) & Recovery Point Objective (RPO)

- Process for monitoring systems (no longer compromised, working as expected)
- Measures to prevent similar incidents

Create recovery plans for different scenarios

7. Lessons Learned

Timing: Within few days of incident

Questions to Answer:

- What exactly happened and at what times?
- How well did staff and management handle incident?
- Were documented procedures followed? Were they adequate?
- What information was needed?
- Have any steps/actions hindered recovery?
- What would staff/management do differently next time?
- How could information sharing with other organizations be improved?
- What corrective measures can prevent similar incidents?
- What precursors/indicators should be watched for?

Benefits:

- Training material for new team members
- Shows experienced team member responses
- Identifies missing steps/inaccuracies in procedures
- Drives policy and procedure updates

Testing Importance:

- Regular testing of CIRP ensures documents remain current
- Testing methods: discussion or functional exercises
- Test scenarios provide valuable lessons learned information
- Adjust procedures and processes based on test outcomes

6. NETWORK SECURITY POLICY

Purpose

Network security is the first defense against outside attacks. Effective measures prevent:

- Infrastructure mapping by cybercriminals
- Communication disruption
- Unlawful data gathering
- Reaching critical applications and devices

Physical Security

Requirements:

- Network components (firewalls, switches) located in dedicated cabinets
- Restricted access to specially designated personnel
- Data and power cables protected from damage

Network Segregation

Purpose: Prevent malware and abuse spreading across network

Design: Segregated topology with systems in designated VLANs separated by firewall access rules

VLAN Segregation Rules:

Requirement	Description
Online Services	Systems providing online services (accepting incoming internet traffic) separated from other systems
Network Management	Via separate VLAN
Connected Services	Systems accepting incoming traffic from untrusted networks (non-internet) separated from other systems
End-user Devices	Separated from servers
Unmanaged Devices	Separated from managed devices
Different Purposes	Systems with different purposes separated
Physical Locations	Physical locations separated
Development Environments	Development, testing, and production systems separated

Firewalling

Requirements:

- VLANs separated by firewalls
- Network traffic between VLANs and to/from untrusted networks blocked unless explicitly required
- Outbound internet access for office user VLANs allowed unless adversely affecting security/performance
- Traffic prioritization possible (prevent video/music streams affecting work traffic)

VPN

Purpose: Encrypt network traffic over untrusted networks for:

- Teleworking
- Machine-to-machine communication

Access Requirements:

- VPN access configured with Multi-Factor Authentication where possible
- Prevents unauthorized persons with compromised credentials from using VPN

Securing Wired Networks

Requirement: Network ports protected from untrusted devices

When Physical Security is Low:

- Use network security techniques:
  - MAC filtering
  - Network access security
- Block or isolate untrusted devices

Wireless Network Security

Wi-Fi Encryption/Authentication Standards (ordered by security - best first):

1. **WPA2 + AES** (only secure method)
2. **WPA + AES** (not preferred)
3. **WPA + TKIP** (not preferred)
4. **WEP** (never use)
5. **Open Network** (never use)

User Access Requirements:

- User access verified
- Central user database by name preferred for authentication
- Most corporate WiFi access points provide LDAP or RADIUS support

Unmanaged Devices:

- Only allowed access to **[dedicated guest WIFI networks]**
- Network traffic between guest networks and managed networks prevented

Network Management

Requirements:

1. **Network Diagram**
   - High-level network diagram developed and stored securely (printed)
   - Includes: hardware, function description, necessary (IP) addressing
   - Updated regularly
1. **Management Ports**
   - Restricted to authorized personnel

- Not connected to internet unless via VPN
- User access monitored regularly
- Central user database by name preferable for authentication

1. **Installation/Modification**
   - Network devices installed/modified by or in consultation with **[Organization]** IT
1. **Logging**
   - Network infrastructure devices feature logging
   - Focus: monitoring and controlling traffic flows through network zones and different trust levels
   - Examples: important administrator events (login, system changes, password resets)
1. **Service Level Agreements (SLAs)**
   - Consider SLAs for network components to ensure availability and performance of critical/confidential systems

7. PASSWORD POLICY

Purpose

Provides policy for use and implementation of passwords for confidential and critical information systems.

Modern Philosophy:

- Long but user-friendly passwords
- Multi-factor authentication strongly encouraged (work and personal accounts)
- Away from: strong passwords changed often

Password Settings

Password Strength

Purpose: Reduce chances of misuse

Password Systems Must Enforce:

Requirement	Rule
Minimum Length	Minimum **X** characters (X recommended)
Administrator Passwords	Minimum **XX** characters
Service Account Passwords	Minimum **XX** characters
Very Long Passwords	Allowed (e.g., 256 characters)
Username Rejection	Passwords containing username rejected
Name Rejection	Passwords containing first or last name rejected

Complexity	Must contain at least three of: Uppercase letters (A-Z), Lowercase letters (a-z), Digits (0-9), Special characters (!@#$%^&*())

Exceptions - 4-Digit Code Allowed When:

- Code is addition to physical access ID (smart card or token)
- System not connected to network with strong physical security controls
- To unlock screen of **[Organization]** mobile device (smartphone or tablet)

Password Change Policy

Purpose: Reduce risk of compromising passwords through regular changes

Requirements:

Requirement	Rule
Default Passwords	Changed for new devices
User-Initiated Changes	Systems allow users to change passwords anytime
Periodic Changes Based on Length	When minimum allowed password length is **X** characters: change every **X** months (or **XX** days)
	When minimum allowed password length is **XX** characters: change every **X** months (or **XX** days)
Third-Party Provided Passwords	Changed at first login (e.g., from ICT department)
Password Reuse	Systems explicitly deny reuse of at least last **X** passwords
Shared Passwords	Changed when people knowing them leave organization

Exceptions - Change Policy Recommended But Not Mandatory When:

- Password used for service account and cannot be used for interactive login
- Code is addition to physical access ID (smart card or token)
- System not connected to network with strong physical security controls
- To unlock screen of **[Organization]** mobile device (smartphone or tablet)

Prevention of Attacks

Requirement: At least one mechanism to prevent brute force attacks

Techniques Examples:

1. **Account Lockout**
    - Disables login functionality for specific account
    - Example: Lock account for **XX** minutes after **X** failed login attempts
1. **Black IP List**
    - Detects failed login attempts by IP address
    - Blacklists IP address after too many attempts (e.g., 20)
1. **Login Delay**
    - Adds incremental repeat delay after wrong password

    - Example: 0.5 sec after 2 failures, 1 sec after 3rd, 2 sec after 4th, 4 sec after 5th, etc.

Password Protection

Requirements:

- **Never share** passwords with anyone (including supervisors and colleagues)
- Treat all passwords as sensitive, confidential **[Organization]** information
- **Never include** in email messages or other electronic communication
- **Never communicate** by phone
- **Only store** in organization-authorized password managers
- **Avoid** passwords on paper unless strong physical security (safe)
- **Do not use** "Remember password" feature of applications (web browsers)
- **Report and change** passwords suspected of compromise

Distribution via Email

Allowed When:

- No external email system used
- Email sent encrypted (like Office 365)
- Username/password combination expires after first use OR after **1 month** if not used

Distribution via SMS

Not Allowed: Never send username and password combinations via SMS

SMS Can Be Used For Partial Login Information When:

- Message contains at most only one part of combination (system, username, password, or token)
- Other parts sent via other distribution methods
- User expects message and likely to use soon
- Information expires after first use OR after 1 month if not used

8. VULNERABILITY AND PATCH MANAGEMENT POLICY

Purpose

Eliminate known vulnerabilities through good patch management system and vulnerability monitoring.

Context:

- Vulnerability = flaw/weakness in design or implementation that can compromise security

- More than 90% of malware infections or cybercrimes start with exploiting known leak
- Systems allowing incoming internet connections face numerous attacks daily

Managing Vulnerabilities

Risk Assessment

- **[Organization]** conducts annual risk assessment
- Determines risk based on: threats, vulnerabilities, impacts on business processes and assets
- Vulnerabilities = weakness in hardware, software, or procedures

Scanning for Internal Vulnerabilities

Frequency by System Criticality:

System Level	Scan Frequency
Critical and Confidential Systems	At least **annually**, **quarterly**, or **continuously**
Highly Critical and Highly Confidential Systems	At least **monthly**

Tools:

- Vulnerability scanning tools or penetration tests
- Contain database of known vulnerabilities
- Can scan single system or entire network
- Note: Only scan vulnerabilities they have access to (firewalls may block some)

Risk Classification:

- Tools classify weaknesses into different risk levels
- Highest risk: Vulnerability exploitable from internet
- Lower risk: Vulnerability usable by infected system to spread malware

Scanning for External Vulnerabilities

Frequency: Annually, **quarterly**, or **continuous scanning**

Purpose:

- External vulnerability scan (pen test) performed
- Results form basis for vulnerability improvement plan (annual, 6-monthly, or monthly)
- Serves as independent measure of system security

IDS/IPS (Intrusion Detection/Prevention Systems)

Purpose:

- While vulnerability scanners detect potential risks
- IDS/IPS provide real-time network monitoring for malicious actions

- IDS: Sends alert when suspicious behavior noticed
- IPS: Takes action (e.g., blocking traffic in firewall)

Consideration: For critical/confidential systems if risk outweighs cost

CVDP - Coordinated Vulnerability Disclosure Policy

Requirement: For organizations pursuing CyFun assurance level **Important** or **Essential**

Definition: Set of predetermined rules allowing participants ("ethical hackers") with good intentions to:

- Detect possible vulnerabilities in systems
- Provide relevant information about them

Must Include:

- Legal framework for cooperation
- Guarantee confidentiality of exchanged information
- Frame disclosure of vulnerabilities (responsible and coordinated manner)
- Made public (usually on website)

Reference: Guide on Coordinated Vulnerability Disclosure Policy by Centre for Cybersecurity Belgium

Patch Management

Requirements:

Item	Frequency	Notes
Managed Servers, Firewalls, Switches, Clients	At least every **2 months**	Unless explicitly decided otherwise
Security Patches	As soon as possible	Only after thorough impact analysis
Security Patch Awareness	Continuous	Must have system/process to know available and applicable patches

Scope:

- Operating systems
- Server software (databases and services)
- Applications

Exception: If system unable to apply security patches despite known vulnerabilities:

- Isolate from internet and internet-connected systems
- Physically secure

Policy Document Interconnections

These policies reference and support each other:

Master Policy:

- **Cybersecurity Policy** - References all other policies as supporting documents

Supporting Policies:

- **Access Control Policy** - Referenced by: Cybersecurity Policy, Asset Management Policy
- **Asset Management Policy** - References: Access Policy, Password Policy, Network Security Policy, Backup Policy, Vulnerability/Patch Management Policy, Cyber Incident Response Plan
- **Backup and Recovery Policy** - Referenced by: Cybersecurity Policy, Asset Management Policy
- **Cyber Incident Response Plan** - Referenced by: Asset Management Policy
- **Network Security Policy** - Referenced by: Cybersecurity Policy, Asset Management Policy
- **Password Policy** - Referenced by: Access Control Policy, Asset Management Policy
- **Vulnerability and Patch Management Policy** - Referenced by: Cybersecurity Policy, Asset Management Policy

Implementation Notes

For All Policies:

1. **Customization Required:**
    - Replace all **[Organization]** placeholders with actual organization name
    - Replace all **[X]**, **[XX]** placeholders with specific values
    - Replace all **[Function]**, **[Person Responsible]** with actual roles/names
    - Green sample text is for example purposes only - must be customized
1. **Document Control:**
    - All policies include document control tables for:
        - Author
        - Owner
        - Date created
        - Last revised by
        - Last revision date
    - All policies include version management tables
1. **Assurance Levels:**
    - Some policies indicate requirements for different CyFun assurance levels:
        - **Basic**

        - **Important**
        - **Essential**
    - Higher levels include all requirements of lower levels plus additional requirements
1. **Regular Review:**
    - All policies should be reviewed and updated regularly
    - Changes must be approved per documented approval process
    - Version control maintained
1. **Training and Awareness:**
    - All personnel must be familiar with relevant policies
    - Regular training and awareness programs required
    - Compliance monitoring necessary
1. **Integration:**
    - Policies designed to work together as comprehensive framework
    - References between policies create cohesive security posture
    - All policies should be accessible and known to relevant personnel

Key Takeaways

This comprehensive cybersecurity policy framework provides:

1. **Holistic Security Coverage:** Addresses all key aspects of organizational cybersecurity
2. **Standards-Based:** Aligned with ISO 27002, CIS Controls v8, IEC 62443, NIST, and EU regulations
3. **Scalable:** Applicable to organizations of different sizes and maturity levels
4. **Practical:** Includes templates, forms, checklists, and examples
5. **Compliance-Ready:** Addresses GDPR, NIS2, and other regulatory requirements
6. **Interconnected:** Policies reference and support each other for comprehensive coverage
7. **Actionable:** Provides specific requirements, procedures, and implementation guidance
8. **Continuous Improvement:** Emphasizes regular review, testing, and lessons learned

Organizations implementing this framework should customize all templates to their specific needs, resources, and risk profile while maintaining the core security requirements outlined in each policy.