

Below is an example of the sort of policy that may suit the proposed design of ResilientIntellect's EU unit, heavily inspired by NIST, ISO27000 and DORA.

1. Identity and Access Management

- Multi-Factor Authentication (MFA) is mandatory for all systems
- Phishing-resistant MFA is required for privileged and administrative accounts
- Access decisions are based on:
 - User identity
 - Device security posture
 - Session location
- Sharing account credentials between staff or non-staff is prohibited
- Passwords should immediately be reset if a user suspects their password has been compromised

2. Hybrid Work and BYOD Security

- Personal devices may only access ResInt systems if enrolled in approved security controls updated to the latest appropriate version
- Devices must:
 - Run supported operating systems (Windows, Mac, Linux-based OS)
 - Be encrypted
 - Never be shared with non-staff or non-IT staff
- Public Wi-Fi access requires Zero Trust secure access and encrypted communication
- Local storage of sensitive data on personal devices is prohibited

3. Cloud and SaaS Security

- All SaaS platforms must be hosted in EU-approved regions
- Secure configuration baselines must be enforced using Cloud Security Posture Management (CSPM)
- Logs from cloud services must be centrally collected into a SIEM
- Cloud access is controlled through identity-based Zero Trust policies

4. AI and Machine Learning Security

- AI training data must be validated and sanitised prior to use
- Access to AI models and datasets is restricted to authorised personnel
- CI/CD pipelines must include:
 - Dependency scanning
 - Code integrity checks
 - Model integrity validation
- Protection against data poisoning and unauthorised model modification is mandatory
- AI must never have the final say on 'important matters'
 - Accounts or data can be suspended but cannot be deleted without human oversight

5. Important Compliance

5.a DORA Compliance

- In compliance with DORA Major ICT-related incidents must be:
 - Logged
 - Assessed
 - Reported to financial supervisory authorities
- Root cause analysis and remediation actions are mandatory

5.b NIS2 Compliance

- Significant cybersecurity incidents must be reported to national authorities:
 - Early warning within 24 hours
 - Incident notification within 72 hours
 - Final report within one month

6. Business Continuity and Operational Resilience

- Backup and recovery procedures must be tested regularly
- Critical systems (AI data, source code repositories) must have:
 - Encrypted backups
 - Geographically separated recovery locations
- Disaster Recovery and Business Continuity Plans must align with DORA resilience requirements

7. Training and Awareness

- Mandatory security awareness training for all staff
- Role-specific training for developers, analysts, and administrators
- Management training on regulatory responsibilities under DORA and NIS2

8. Enforcement

- Non-compliance with this policy may result in:
 - Disciplinary action
 - Referral to additional training courses
 - Revocation of system access

9. Policy Review

- This policy will be reviewed:
 - Bi-annually
 - After significant incidents that disrupt business or otherwise urge review
 - Following regulatory changes
 - Following changes in managerial staff