PERPETUUM
CAPITAL

Your ultimate guide to the ISO 27001 Policy desk

The absolute must haves (start with these)

1. Information Security Policy
2. Risk Management Policy (containing also info on risk assessment and risk treatment)
3. Statement of Applicability (technically *not a policy*, but absolutely essential)
4. Information Classification Policy
5. Acceptable Use Policy
6. Incident Management Policy
7. Supplier Security Policy

Give it purpose and understanding: Policies to "manage" your ISMS

1. Business Continuity and Backup Policy
2. Access Control Policy
3. Asset Management Policy
4. Information Security Awareness and Training Policy
5. Clear Desk and Clear Screen Policy
6. Remote Working Policy
7. System Acquisition, Development and Maintenance
8. Cryptographic Controls Policy
9. Logging and Monitoring Policy
10. Server (Data Center) Room Concept
11. List of Legal, Regulatory, Contractual and other requirements

The Polishing: Connect the dots and "live" it

1. Procedures for Internal Audit
2. Procedure for Corrective Action
3. Data Protection and Data Retention Policy
4. Continual Improvement Policy
5. Network Security & Secure Development Policy
6. NDAs
7. Management Review
8. KPIs

TOTAL: 26

By meticulously crafting and implementing the comprehensive suite of policies outlined in this ISO 27001 Policy desk, you not only establish a robust foundation for Information Security Management but also instill a culture of proactive risk mitigation, regulatory compliance, and continual improvement, ensuring the resilience and integrity of your organization's information assets.

e-Mail: ka@pcapital.ch | **Web**: www.pcapital.ch