Privacy and Security Measures

Policies and Procedures

1. **Purpose:** Define guidelines, standards, and controls to effectively mitigate risks.
2. **Key Policies:**
    - **Information Security Policy:** Outlines information security management standards.
    - **Data Protection Policy:** Focuses on safeguarding privacy and ensuring compliance with relevant regulations.
    - **Business Continuity Plans:** Ensuring operational continuity during and after disruptions.
    - **Incident Response Policy:** Details methods for detecting, reporting, and resolving security breaches, including requirements to notify authorities.
    - **Mandatory Compliance:** Applies to all personnel, including external contractors.
    - **Review & Update:** Conducted regularly to maintain the effectiveness and relevance of policies.

Awareness and Training

1. **Purpose:** Provide personnel with the knowledge necessary to uphold security and privacy standards.
2. **Key Components:**
    - Annual, role-focused training sessions.
    - Ongoing support and guidance on security practices and data protection.
    - Instructions on maintaining confidentiality obligations and data privacy.

Confidentiality Controls

1. **Physical Access Control:** Protect facilities from unauthorized entry.
    - **Technical:** Electronic access systems, reinforced doors, surveillance cameras, etc.
    - **Organizational:** Access reviews and role-based permissions.
2. **Logical Access Control:** Prevent unauthorized system usage.
    - **Technical:** Strong passwords, firewalls, VPNs, encryption, and two-factor authentication.
    - **Organizational:** User permission management, adherence to least privilege principles, and periodic reviews.
3. **Authorization Control:** Restrict data access based on specific roles.
    - **Technical:** Robust authentication methods.
    - **Organizational:** Role-based access assignments and minimal administrative accounts.
4. **Separation Control:** Ensure data intended for different purposes is processed separately.
    - **Technical:** Logical and physical system segmentation.
    - **Organizational:** Clearly defined database permissions and controlled environments.

Integrity Controls

1. **Transfer Control:** Secure data during transmission.
    - **Technical:** Encrypted connections and logging systems.
    - **Organizational:** Monitoring and oversight of data transfers.
2. **Input Control:** Track and record data alterations.
    - **Technical:** Logging mechanisms and automated log reviews.

- **Organizational:** Assigned responsibilities and traceable actions.

Availability and Resilience

1. **Availability Control:** Protect data from loss.
    - **Technical:** Fire prevention systems, uninterruptible power supplies (UPS), RAID configurations, and environmental monitoring.
    - **Organizational:** Established backup routines and emergency plans.
2. **Recoverability Control:** Restore data following incidents.
    - **Technical:** Regular backups and automated recovery solutions.
    - **Organizational:** Testing recovery procedures and storing backups offsite.

Data Protection Management

1. Centralized documentation of all relevant regulations and obligations.
2. Incorporation of privacy by design and by default.
3. Defined processes for managing data subject access requests.

Incident Response Management

1. **Purpose:** Respond promptly and effectively to security breaches and data loss events.
2. **Key Practices:**
    - Use up-to-date firewalls, spam filters, and virus scanners.
    - Engage with data protection experts when necessary.
    - Document all incidents and ensure thorough follow-up actions.