IT Security Audit Checklist for Compliance with GDPR

Ensure your organization adheres to data protection regulations with this comprehensive **IT security audit checklist** tailored for GDPR compliance. It covers key areas such as access controls, data encryption, and breach response protocols. Regular audits help identify vulnerabilities and maintain robust security standards.

Checklist Items

- **Data Inventory & Classification**
  - Identify and document all personal data processed.
  - Classify data according to sensitivity.
- **Access Controls**
  - Implement role-based access control (RBAC).
  - Review user access privileges regularly.
  - Use strong authentication methods (e.g., MFA).
- **Data Encryption**
  - Encrypt personal data at rest and in transit.
  - Ensure encryption keys are securely managed.
- **Data Minimization & Retention**
  - Collect and process only data necessary for the stated purpose.
  - Implement data retention and secure deletion policies.
- **Security Incident & Breach Response**
  - Maintain a documented incident response plan.
  - Test breach detection and response processes regularly.
  - Ensure breach notification protocols align with GDPR requirements.
- **Third-party Management**
  - Assess the GDPR compliance of vendors and processors.
  - Maintain up-to-date data processing agreements.
- **User Rights & Consent Management**
  - Establish procedures for managing data subject requests (access, rectification, erasure, portability).
  - Implement clear consent mechanisms and records.
- **Training & Awareness**
  - Conduct regular GDPR and security awareness training.
  - Document training attendance and materials.
- **Policy Review & Documentation**
  - Maintain and regularly update security and data protection policies.
  - Keep records of data processing activities.
- **Regular Audits & Assessments**
  - Perform scheduled internal and external compliance audits.
  - Address any identified vulnerabilities promptly.

Note: This checklist should be reviewed and updated regularly to keep up with evolving GDPR requirements and security threats.