DATA PROTECTION CHECKLIST

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken

Data Protection Checklist

1. **Data Classification:**

- [ ] Classify data based on sensitivity and criticality to prioritize protection efforts.
- [ ] Identify and label sensitive data types (e.g., personally identifiable information, financial data).

2. **Access Controls:**

- [ ] Implement role-based access controls (RBAC) to restrict access to sensitive data.
- [ ] Enforce the principle of least privilege to ensure users have access only to the data necessary for their roles.
- [ ] Monitor and log access to sensitive data, including both successful and failed attempts.

3. **Encryption:**

- [ ] Encrypt sensitive data at rest and in transit using strong encryption algorithms (e.g., AES).
- [ ] Implement encryption for data stored in databases, file systems, and backups.
- [ ] Securely manage encryption keys and ensure they are rotated regularly.

4. **Data Masking and Anonymization:**

- [ ] Mask or anonymize sensitive data in non-production environments to reduce the risk of unauthorized exposure.
- [ ] Use techniques such as tokenization or pseudonymization to replace sensitive data with realistic but non-sensitive values.
- [ ] Implement dynamic data masking to restrict access to sensitive data based on user permissions.

5. **Data Loss Prevention (DLP):**

- [ ] Deploy DLP solutions to monitor, detect, and prevent unauthorized data exfiltration or leakage.
- [ ] Configure DLP policies to enforce rules and regulations regarding data protection and privacy.
- [ ] Implement endpoint DLP controls to prevent unauthorized data transfers and leaks from endpoints.

6. **Data Retention and Disposal:**

- [ ] Establish data retention policies to specify how long data should be retained based on legal, regulatory, and business requirements.
- [ ] Regularly review and dispose of data that is no longer necessary or has exceeded its retention period.
- [ ] Ensure proper data disposal methods, including secure deletion and shredding of physical and digital media.

7. Data Backup and Recovery:

- [ ] Implement regular backups of critical data to ensure resilience against data loss or corruption.
- [ ] Store backups securely in off-site or cloud repositories to protect against physical and logical threats.
- [ ] Test backup and recovery procedures periodically to verify data integrity and availability.

8. Data Privacy Compliance:

- [ ] Ensure compliance with relevant data protection regulations (e.g., GDPR, CCPA) and industry standards.
- [ ] Conduct privacy impact assessments (PIAs) to identify and mitigate privacy risks associated with data processing activities.
- [ ] Maintain records of data processing activities, legal bases, and consent mechanisms to demonstrate compliance.

9. Employee Training and Awareness:

- [ ] Provide comprehensive training and awareness programs to educate employees about data protection policies and procedures.
- [ ] Conduct regular security awareness sessions to reinforce best practices for handling sensitive data.
- [ ] Foster a culture of security and privacy awareness across the organization through ongoing communication and training.

10. Incident Response and Reporting:

- [ ] Develop and maintain an incident response plan outlining procedures for detecting, reporting, and responding to data breaches.
- [ ] Establish a designated incident response team responsible for managing data breach incidents.
- [ ] Notify affected individuals and regulatory authorities promptly in accordance with legal requirements and regulations.

https://ie.linkedin.com/in/hanimeken

11. Vendor and Third-Party Risk Management:

- [ ] Assess and vet vendors and third-party service providers for their data protection practices and security controls.
- [ ] Include data protection requirements in vendor contracts and agreements to ensure compliance and accountability.
- [ ] Monitor and audit third-party access to sensitive data to prevent unauthorized exposure or misuse.

12. Continuous Improvement and Review:

- [ ] Conduct regular risk assessments and audits to identify vulnerabilities and gaps in data protection controls.
- [ ] Continuously monitor and update data protection measures to address emerging threats and compliance requirements.
- [ ] Establish a process for feedback and improvement based on incidents, audits, and lessons learned.

HANIM EKEN

https://ie.linkedin.com/in/hanimeken