Backup Policies for Ransomware Resilience

General Data Backup Policy

Objective: Ensure regular backups of critical data to minimize the impact of ransomware or other data loss incidents.

1. Backup Frequency:
   - Perform daily backups of critical systems (e.g., financial data, customer databases).
   - Weekly full-system backups for non-critical systems.

2. Backup Types:
   - Use incremental backups for daily operations.
   - Perform a full backup every weekend or on a defined schedule.

3. Storage Locations:
   - Maintain 3 copies of all backups:
     - 1 primary copy on the operational system.
     - 1 backup copy stored on an offline external drive.
     - 1 backup copy stored in a secure cloud environment.

4. Access Controls:
   - Restrict access to backup systems to authorized personnel only.
   - Enforce multi-factor authentication (MFA) for accessing backup systems.

5. Testing and Validation:
   - Test backup restoration processes monthly to ensure functionality and data integrity.
   - Perform annual audits of backup procedures.

6. Retention Policy:
   - Retain daily backups for 30 days.
   - Retain weekly backups for 3 months.
   - Retain monthly backups for 1 year.

7. Encryption:
   - Encrypt all backup data, both in transit and at rest, using strong encryption algorithms (e.g., AES-256).

8. Ransomware Considerations:

   - Ensure at least one backup copy is immutable (cannot be altered) or air-gapped (disconnected from the network).

Cloud Backup Policy

Objective: Secure and manage backups stored in cloud environments to prevent ransomware attacks on backup data.

1. Service Selection:
   - Use reputable cloud storage providers with high security standards.

2. Backup Automation:
   - Automate backup processes to reduce the risk of human error.

3. Access Management:
   - Configure role-based access controls (RBAC) to limit who can access cloud backups.

4. Snapshot Retention:
   - Configure frequent snapshots (e.g., hourly for critical data).

5. Disaster Recovery Planning:
   - Include cloud backups in the organization's disaster recovery plan.

6. Monitoring and Alerts:
   - Set up alerts for unusual activities, such as bulk deletion or unauthorized downloads of backups.

Offline Backup Policy

Objective: Maintain offline backups as a last resort for ransomware recovery.

1. Frequency:
   - Perform weekly offline backups for critical systems.

2. Storage Medium:
   - Use high-capacity external drives or tape storage systems.

3. Access Restrictions:
   - Assign backup creation and retrieval responsibilities to a small, trusted team.

4. Rotation Policy:
   - Rotate offline backups weekly to ensure at least two recent copies are available.

5. Testing:
   - Test offline backups quarterly to verify their usability.

Ransomware-Specific Backup Policy

Objective: Harden backups against ransomware attacks and ensure a seamless recovery process.

1. Immutable Backups:
   - Configure at least one backup copy as immutable.

2. Air-Gapped Backups:
   - Store backups on devices disconnected from the network (air-gapped storage).

3. Rapid Recovery Protocol:
   - Create a recovery playbook detailing steps to restore data from backups.

4. Backup Monitoring:
   - Implement real-time monitoring of backup activities to detect anomalies.

5. Backup Integrity Checks:
   - Run automated checks to verify the consistency and integrity of backup files.