4.12.1 Backup and Recovery Management

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this “Backup and Recovery Management policy” the following definitions apply:

- **Backup:** a copy of data or information assets created as a safeguard against data loss, corruption, or system failures.
- **Online Backup:** the process of copying and storing data on remote servers or cloud-based platforms.
- **Offline Backup:** also known as offline storage, involves storing backup copies of data on physical media or devices (e.g., tapes, external hard drives, or offline storage systems). These backups are kept in a secure, isolated environment.
- **Retention Period:** specifies the length of time that backup data is retained before it is overwritten or deleted.
- **Rapid Recovery:** Rapid recovery refers to the ability to quickly restore critical systems and data following a cybersecurity incident or system failure. It minimizes downtime and disruption to business operations.
- **Backup Validation:** the process of regularly testing and verifying the integrity and recoverability of backup copies.
- **Encryption:** the process of converting event log data into a secure and unreadable format to protect it from unauthorized access during transmission or storage. This ensures the confidentiality and integrity of sensitive log information.
- **Access controls:** the mechanisms and policies implemented to manage and regulate access to a system or network. These controls ensure that only authorized individuals or systems can access specific resources, data, or functionalities.

2. Purpose

The purpose of this Backup and Recovery Policy is to define and document the requirements for the management of backup and recovery processes to ensure the availability, integrity, and rapid recovery of information assets, as well as protection against cybersecurity incidents.

3. Scope

The scope of the Backup and Recovery Policy encompasses the management of online and offline backups, specifying retention periods, rapid recovery procedures for cybersecurity incidents, periodic backups, protection measures, and ensuring the availability of backup data.

4. Policy

4.1. The NOC team shall implement a comprehensive backup process that encompasses both online and offline backups to protect information assets from loss or damage. This includes:
- Regular online backups of critical systems and data.
- Offline backups, stored securely in an isolated environment, to safeguard against data loss due to cybersecurity incidents.
- A defined retention period for online backups 7 days, and for offline backup 1 year.

4.2. To ensure rapid recovery in the event of cybersecurity incidents, the IT operation team shall maintain up-to-date and tested backup copies of critical systems and data, allowing for the swift restoration of services and operations.

4.3. Backup and recovery process must be specified to minimize data and system recovery time in the event of a cybersecurity incident.

4.4. Information assets, including databases, configurations, and critical data, shall be backed up periodically according to a defined schedule.

4.5. Backup frequencies shall be determined based on business needs, data criticality, and regulatory requirements.

4.6. Backups shall be stored in a secure and physically controlled environment to prevent unauthorized access and tampering.

4.7. Backup shall be encrypted to protect the confidentiality and integrity of stored data.

4.8. Access controls and audit trails shall be implemented for individuals authorized to perform backup and recovery operations.

4.9. Backup and recovery procedures shall ensure the availability of backups when needed.

4.10. Backup data shall be regularly monitored to detect any corruption or anomalies, and corrective actions shall be taken promptly.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards
- NIST