Module 2: Backup Strategies and Planning

2.0 What are Backup Strategies?

Backup strategies involve designing and implementing a comprehensive plan to safeguard data against loss, corruption, or accidental deletion. A well-defined strategy ensures:

- **Data Recovery**: Reliable and swift recovery during disasters or data breaches.
- **Business Continuity**: Minimal downtime, ensuring operations remain uninterrupted.
- **Regulatory Compliance**: Meeting legal and industry requirements for data storage and retention.

Key aspects of a backup strategy include:

- **Critical Data Identification**: Pinpointing essential data to back up.
- **Backup Types**: Full, incremental, differential, or hybrid.
- **Storage Options**: Local, external, network-attached, or cloud-based solutions.
- **Testing and Validation**: Regular checks to ensure recoverability.

2.1 Identifying Critical Data to Backup

Identifying the most critical data to back up ensures maximum protection for essential operations.

1. Websites

- Dynamic website files, such as HTML, CSS, JavaScript, and media assets.
- Content management systems (CMS), plugins, themes, and custom code.

- System logs and error logs for troubleshooting and auditing purposes.

2. Databases

- Data tables, schemas, stored procedures, and application data.
- Backup tools: MySQL Dump, phpMyAdmin export, or automated scripts.

3. Emails

- Important emails stored on servers (e.g., IMAP, POP3).
- Account configurations and settings.
- Email backups from platforms like SmarterMail, cPanel, or any other email solutions.

4. Configurations

- Web server configurations
- Application settings (Example **.env** files, **configuration.yaml**).
- SSL certificates, API keys, DNS records, and security credentials.

2.2 Frequency and Retention Policies

1. Backup Frequency

Backup schedules should align with the frequency of changes in the data:

- **Daily Backups**: For transactional databases, emails, and frequently updated files.
- **Weekly Backups**: For moderately updated systems, like static content.
- **Monthly Backups**: For archives, historical records, or compliance purposes.

2. Retention Policies

Retention policies determine how long backups are stored:

- **Short-Term**: Retain daily backups for 7–14 days for operational needs.
- **Mid-Term**: Retain weekly backups for 4–8 weeks for recovery from extended issues.
- **Long-Term**: Retain monthly backups for up to 7 years for compliance or archival purposes. Not applicable for Truehost
- For more details on Backup retention, refer to terms of service for Truehost.

Compliance and Recovery

- Align retention policies with legal requirements (e.g., GDPR, DPA-The Data Protection Act (DPA) of 2019).
- Periodically audit policies to reflect evolving regulatory and business needs. For example, Truehost used to keep 7 most recent daily backups. This was revised to 5 most recent daily backups.
- Maintain backups that support **Recovery Point Objective (RPO)** and **Recovery Time Objective (RTO)**. For example, Truehost configures backups for all accounts such that should there be a need for migration, it the recovery takes the least time possible.

2.3 Backup Storage Options

Selecting the right storage option is essential for backup reliability and security.

1. Local Storage

- **External Drives**: Portable hard drives for offline backups. You can generate your full account backups (cPanel, Plesk, Cyberpanel, CWP) and store them locally on external drives.
- **Network-Attached Storage (NAS)**: Centralized storage accessible over a local network. You can upload your website backups here for safekeeping and should need arise, you can download them and upload to your server.

- Pros: Fast access, high control.
- Cons: Vulnerable to physical damage or theft.

2. Cloud Backup Services

- Providers: AWS S3, Google Drive, Dropbox, and Azure Backup backup as a service
- Features: Automated backups, scalability, and off-site storage.
- Pros: Remote access, redundancy, and advanced security.
- Cons: Recurring costs and dependency on internet connectivity.

3. Hybrid Solutions

- Combine local and cloud backups for enhanced redundancy and availability.
- Example: Daily backups to a NAS and monthly backups to the cloud.

2.4 Risk Assessment and Testing

A backup strategy is incomplete without evaluating potential risks and testing recovery processes.

1. Risk Assessment

- Identify vulnerabilities such as hardware failure, cyberattacks, or accidental deletion.
- Ensure backups are stored in locations safe from natural disasters (e.g., fires, floods).

2. Simulating Disaster Recovery Scenarios

- Perform mock disaster recovery tests to validate restoration workflows.
- Scenarios: Server crashes, ransomware attacks, or accidental file deletions.

3. Verifying Backup Integrity

- Regularly check backup files to ensure they are not corrupted.
- Use checksum verification or other integrity testing tools.

4. Documenting Results

- Maintain logs of tests and risk assessments.
- Use insights from testing to optimize the backup strategy and mitigate future risks.