Chameleon
Security

Data Backup Policy

1. **Purpose**

   The purpose of this data backup policy is to establish guidelines for the backup and recovery of critical data for Chameleon Company. The policy is designed to ensure the protection and availability of data in the event of accidental loss, corruption, hardware failure, cyber-attacks, or natural disasters. Implementing a robust backup strategy is crucial for maintaining data integrity and business continuity.

2. **Backup Strategy**

   Chameleon will adopt a multi-tiered backup strategy to ensure data redundancy and mitigate the risk of data loss. The strategy will include regular backups of critical data, secure storage of backup copies, encryption of backup data, periodic testing of backups, and clear documentation of backup procedures. The backup strategy will be aligned with industry best practices and compliance requirements to safeguard the organization's data assets.

3. **Procedures**

   a. Identification of Critical Data: The IT department will collaborate with data owners to identify crucial data that are required to be backed up, encompassing databases, applications, files, and other essential operational data.
   b. Backup tools: Chameleon will provide reliable backup tools and software to facilitate the backup process. Backup solutions will be chosen based on scalability, efficiency, and compatibility with the organization's IT infrastructure.
   c. Backup Methodology: Regular backups will be performed on a daily basis to capture incremental changes in data. Weekly full backups will also be conducted to ensure comprehensive data protection. Backup processes will be automated to minimize human errors and ensure consistency.
   d. Encryption of Backup Data: Industry-standard encryption algorithms will be used to encrypt all backup data, preventing unauthorized access and maintaining data confidentiality. The management of encryption keys will be conducted securely to protect backup copies.
   e. Testing: The company will conduct quarterly backup tests to verify the integrity of the backup data and the restoration process. Testing will include both incremental and full backups to validate the entire backup infrastructure.
   f. Monitoring: Chameleon will implement automated monitoring tools to track the status of backups and generate alerts in case of any issues. IT personnel will review backup logs regularly to ensure that backups are performed successfully.
   g. Storage of Backup Data: Backup copies will be stored in multiple locations, including on-site and off-site storage facilities. On-site backups will enable quick recovery in the event of minor incidents, while off-site backups will provide protection against catastrophic events such as fires, floods, or earthquakes.

4. **Backup Schedule:**

   - Daily Incremental Backups: Backups will be performed daily to capture changes in data throughout the day.

- Weekly Full Backups: Full backups will be conducted once a week to ensure that all data is backed up in its entirety.
- Regular Testing: Quarterly testing of backups will be conducted to verify the integrity of backup copies and the effectiveness of the restoration process.

5. **Data Recovery**

   In the event of data loss, the IT department will be responsible for initiating data recovery procedures. Data recovery will be conducted based on the established backup schedule and retention policy. The recovery process will aim to restore data to its latest available state to minimize operational disruptions.
6. **Data Retention:** Backup copies will be retained for a minimum period of 30 days to facilitate data recovery in case of accidental deletion or corruption. Backup data older than 30 days will be archived for long-term storage purposes. Archived backups will be retained for a minimum period of one year to meet compliance requirements and facilitate historical data retrieval.
7. **Compliance**

   This data backup policy applies to all employees, contractors, and third parties who have access to company data. It covers all types of data stored on company-owned devices, servers, cloud services, and any other storage medium used by the organization. Compliance with the backup policy is mandatory for all personnel involved in managing and handling organizational data.
8. **Training and Awareness**

   Regular training and awareness programs will be conducted to educate employees on the importance of backups and data protection. All employees will receive training on backup procedures, data retention policies, and disaster recovery strategies. Employees will be informed about the roles and responsibilities related to backups and data security.