

# Data Storage and Access Controls Format

## 1. Document Information

Document Owner: \_\_\_\_\_

Version: \_\_\_\_\_

Date: \_\_\_\_\_

Department: \_\_\_\_\_

## 2. Data Storage Details

Data Type	Storage Location	Format	Data Sensitivity
Customer Records	Secure Cloud Database	Encrypted SQL	Confidential
Transaction Logs	Internal File Server	CSV	Internal
Audit Trails	Third-party Audit Platform	JSON	Sensitive

## 3. Access Controls

Role/User Group	Access Level	Authentication Method	Approval Required
Admin	Full Access	2FA & Password	Yes
Data Analyst	Read Only	Single Sign-On	Yes
Support Staff	Limited	Password	No

## 4. Data Retention and Backup

- Retention Period: \_\_\_\_\_
- Backup Frequency: \_\_\_\_\_
- Backup Location: \_\_\_\_\_
- Disposal Method: \_\_\_\_\_

## 5. Monitoring & Review Procedures

- Access logs are reviewed: \_\_\_\_\_
- Storage health checked: \_\_\_\_\_
- Compliance audits scheduled: \_\_\_\_\_

## Important Notes

- This format should be reviewed and updated regularly to reflect current data handling practices.
- All storage and access methods should comply with applicable laws and internal policies.
- Ensure only authorized personnel have appropriate access to sensitive data.
- Backup and data disposal methods must be secure and documented.
- Maintain thorough documentation for audit and compliance purposes.