Cloud System Administration SOP

Purpose

To establish secure, efficient, and standardized procedures for administering cloud systems. This includes cloud backups, access control, and system monitoring within Microsoft 365 Business and other cloud services. This SOP applies to all IT personnel responsible for managing the cloud infrastructure, including data backups, account and permission control, and ongoing monitoring of Microsoft 365 and associated services.

1. Cloud Backup Management
2. Data to backup includes SharePoint document libraries, OneDrive user files, Microsoft Teams content, and Exchange Online mailboxes.
3. Automated daily backups should occur daily using a third-party cloud backup service. Retention is one year for general data and seven years for compliance-related data.
4. Monthly test restorations should be conducted to validate data integrity. Document validation results in a backup verification log.
5. In case of major failure or data loss, initiate recovery protocols as defined in the Data Breaches SOP.
6. Access Control
7. All user accounts must be created via the Microsoft 365 Admin Center and assigned appropriate roles. Follow the Deactivation vs. Deletion SOP for user offboarding and access transitions.
8. Regarding permissions, implement role-based access control, grant least privilege necessary for job duties, and use Microsoft Entra ID security groups to manage access to SharePoint, Teams, and other resources.
9. Multi-factor authentication (MFA) must be enabled for all users and passwords must meet complexity standards and expire every 90 days.
10. Quarterly reviews should be conducted for all user and admin accounts. Document findings and adjustments in access review reports.
11. System Monitoring
12. Use Microsoft 365 Admin Center and Microsoft Defender for Office 365 for monitoring. Enable security alerts for anomalous behavior, including but not limited to, multiple failed logins, foreign IP logins, and large file downloads.
13. Enable unified audit logging for Exchange, SharePoint, Teams, and OneDrive. Retain logs for at least 90 days (longer for sensitive accounts).
14. Use the Data Breaches SOP for handling suspected intrusions or service disruptions.
15. Use the Software Deployment SOP and license management tools to track licensing and compliance.
16. Security and Compliance
17. All cloud system operations must adhere to the Sensitive Data Policy.
18. Regular risk assessments must be conducted to evaluate cloud system configurations and vendor compliance.
19. Tools or plugins must be vetted under the Unpaid Tools, Services, and Software Usage SOP.

This SOP must be reviewed annually or following major updates to Microsoft 365 services or internal IT infrastructure.