Authors: [Bradley Baack, Rebecca Childs, Ethan Pham, Cody Blahnik]

SOP 1 - Teamwork Tools Setup - Microsoft Teams and SharePoint

- Objective:

The purpose of this SOP is to provide a standardized process for setting up Microsoft Teams and SharePoint to facilitate efficient collaboration and teamwork within the organization.

- Scope:

This SOP applies to all employees involved in the setup and utilization of Microsoft Teams and SharePoint.

Responsibilities:

- IT Department: Responsible for the initial setup, configuration, and ongoing maintenance of Microsoft Teams and SharePoint.
- End Users: Responsible for following the established procedures for accessing and utilizing Microsoft Teams and SharePoint.

Procedure:

- Microsoft Teams Setup:
- Log in to the Microsoft 365 Admin Center.
- Navigate to the Teams admin center and configure general settings.
- Set up Teams policies, including messaging, meetings, and app permissions.
- Create Teams and channels based on departmental or project needs.

Add and manage users within Teams.

- SharePoint Setup:
- Access the SharePoint admin center in the Microsoft 365 Admin Center.
- Create a new SharePoint site for each team or project.
- Configure site permissions, ensuring proper access for team members.
- Set up document libraries and folders as needed.

Enable versioning and other relevant document control features.

- Integration Between Microsoft Teams and SharePoint:
- a. Link SharePoint sites to corresponding Teams channels.
- b. Configure document collaboration settings within Teams.

Utilize the Files tab in Teams to access and collaborate on SharePoint documents.

- User Training and Communication:
- Develop training materials and documentation for Microsoft Teams and SharePoint usage.
- Conduct training sessions or workshops to familiarize users with the tools.

Communicate any updates or changes to the Teams and SharePoint setup.

- Troubleshooting and Support:
- Establish a process for reporting issues or seeking support related to Teams and SharePoint.
- Maintain a knowledge base or FAQ to address common user concerns.

Provide ongoing support and updates as needed.

- Documentation and Record Keeping:

Maintain documentation of the Teams and SharePoint setup, including configurations, access permissions, and any changes made. Regularly review and update the documentation as needed.

-

Title: SOP 2 - VMware Virtual Machine Management

- Objective:

The objective of this SOP is to establish standardized procedures for the creation, configuration, and management of virtual machines using VMware in the organization.

- Scope:

This SOP applies to IT personnel responsible for the deployment and maintenance of virtual machines within the VMware environment.

Responsibilities:

- IT Department: Responsible for the installation, configuration, and ongoing management of VMware environments.
- System Administrators: Responsible for creating, monitoring, and maintaining virtual machines.

Procedure:

VMware Environment Setup:

- Install and configure the VMware vSphere/ESXi hypervisor on the designated server.
- Configure network settings, storage, and other necessary parameters during the initial setup.

Implement security measures for the VMware environment.

- Datastore Configuration:
- Set up and configure datastores to store virtual machine files.

Monitor datastore capacity, performance, and implement necessary optimizations.

- Virtual Machine Creation:
- Access the vSphere client or web interface.
- Create a new virtual machine, specifying hardware resources (CPU, RAM, storage).
- Install the guest operating system using ISO or other installation methods.

Configure virtual machine settings, including network adapters and storage.

- Cloning and Templates:
- Create templates for commonly used virtual machine configurations.
- Use templates for efficient and consistent virtual machine deployment.

Implement cloning for duplicating virtual machines as needed.

- Networking Configuration:
- Configure virtual networks and port groups.
- Connect virtual machines to the appropriate networks.

Implement network security measures and policies.

- Performance Monitoring:
- Monitor resource usage (CPU, memory, disk, network) of virtual machines.
- Utilize VMware tools for performance analysis.

Address performance issues promptly.

- Snapshot Management:
- Create snapshots before making significant changes or updates.
- Regularly monitor and manage existing snapshots.

Document snapshot usage and retention policies.

- Backup and Recovery:
- Establish regular backup schedules for critical virtual machines.
- Test backup and recovery procedures periodically.

Document backup and recovery processes.

- Security Measures:
- Implement security best practices for virtual environments.
- Regularly update and patch the VMware infrastructure.

Control access to virtual machines and vSphere/ESXi hosts.

- Documentation and Inventory:
- Maintain an inventory of all virtual machines.
- Document configurations, IP addresses, and other relevant details.

Update documentation promptly when changes are made.

-

Title: SOP 3 - File Sharing and Safety - OneDrive and AWS S3

- Objective:

The objective of this SOP is to provide guidelines for secure and efficient file sharing, storage, and collaboration using OneDrive and AWS S3 in the organization.

- Scope:

This SOP applies to all employees using OneDrive and AWS S3 for file storage, sharing, and collaboration.

Responsibilities:

- IT Department: Responsible for the setup, configuration, and maintenance of OneDrive and AWS S3.
- End Users: Responsible for following established procedures for file sharing, storage, and safety.

Procedure:

- OneDrive Setup:
- Access the OneDrive admin console.
- Configure user accounts and permissions.

Define storage quotas and retention policies.

- AWS S3 Setup:
- Access the AWS Management Console.
- Create an S3 bucket for file storage.

Configure access controls, encryption, and versioning.

- File Upload and Sharing:
- Use the OneDrive client or web interface to upload files.
- Share files securely with internal and external users.

Monitor and control access to shared files.

- Version Control:
- Enable versioning for files stored in OneDrive and AWS S3.
- Communicate version control policies to users.

Regularly review and manage file versions.

- Collaboration Tools:
- Utilize collaboration features in OneDrive, such as co-authoring.
- Set up and manage shared folders for team collaboration.

Use AWS S3 features for collaboration, such as bucket policies.

- Security Measures:
- Implement multi-factor authentication for OneDrive and AWS accounts.
- Encrypt sensitive files before uploading to cloud storage.

Regularly review and update access permissions.

- Monitoring and Auditing:
- Monitor file activities and user access logs in OneDrive and AWS S3.
- Conduct periodic audits to ensure compliance with security policies.

Investigate and address any unauthorized access promptly.

- Backup and Recovery:
- Implement regular backup procedures for critical files.
- Test file recovery processes to ensure data integrity.

Document backup and recovery procedures.

- User Training:
- Develop training materials for OneDrive and AWS S3 usage.
- Conduct training sessions to educate users on best practices.

Provide ongoing support and updates as needed.

- Documentation and Record Keeping:
- Maintain documentation of OneDrive and AWS S3 configurations, access controls, and any changes

Title: SOP 4 - Basic Security First

- Objective:

The objective of this SOP is to establish fundamental security practices to safeguard information, systems, and assets within the organization.

- Scope:

This SOP is applicable to all employees, contractors, and third-party individuals with access to the organization's information systems.

- Responsibilities:

All employees and authorized personnel are responsible for understanding and adhering to the basic security measures outlined in this SOP.

Procedure:

- User Authentication:
- Utilize strong and unique passwords for all accounts.

Implement multi-factor authentication (MFA) where available.

- Device Security:
- Keep all devices, including computers, laptops, and mobile devices, updated with the latest security patches.

Enable device encryption to protect sensitive data.

- Email Security:
- Be cautious of phishing emails and verify the legitimacy of email links and attachments.

Use encrypted email for sensitive information.

- Physical Security:
- Ensure physical access controls to secure areas and server rooms.

Lock workstations when leaving them unattended.

- Data Backup:
- Regularly back up critical data and ensure backup integrity.

Test data restoration procedures periodically.

- Security Software:
- a. Install and regularly update antivirus and anti-malware software on all devices.

Use firewalls to control network traffic.

- Access Controls:

- Implement the principle of least privilege, granting users only the minimum access required for their role.

Regularly review and update access permissions.

- Network Security:
- Use secure and encrypted Wi-Fi networks.

Regularly change Wi-Fi passwords and router access credentials.

- Incident Reporting:
- Report any security incidents, including lost devices or suspected breaches, immediately to the IT department.

Follow the organization's incident response procedures.

- Security Awareness Training:
- Conduct regular security awareness training for all employees.

Provide updates on emerging security threats and best practices.

-