SOP: Internal Communication Channels Setup and Access Protocols

This SOP details the setup and management of **internal communication channels**, including the selection of appropriate platforms, configuration of user access protocols, guidelines for secure communication, role-based permissions, and procedures for regular monitoring and maintenance. Its purpose is to ensure efficient, secure, and accessible communication across all departments to enhance collaboration and information sharing within the organization.

1. Purpose

To provide guidelines for establishing, accessing, securing, and maintaining internal communication channels to support effective and compliant communication across all organizational levels.

2. Scope

This SOP applies to all internal communication platforms, including but not limited to email systems, instant messaging applications, internal forums, and collaboration tools utilized by staff in all departments.

3. Responsibilities

Role	Responsibility
IT Department	Select, set up, and maintain communication platforms. Manage access and oversee security protocols.
Department Heads	Identify platform needs, allocate roles and permissions, and enforce usage guidelines.
All Employees	Use communication channels responsibly and securely according to this SOP.

4. Procedure

4.1 Platform Selection

1. Identify communication requirements per department and organization-wide.
2. Evaluate potential communication platforms for security, usability, scalability, and integration.
3. Select platforms (e.g., Microsoft Teams, Slack, Outlook, Google Workspace) that meet organizational standards.
4. Document platform selection and approval.

4.2 Configuration and Setup

1. Install and configure selected platforms as per vendor best practices.
2. Integrate platforms with existing IT infrastructure where necessary.
3. Establish default channels/groups and set naming conventions.

4.3 User Access Protocols

1. Assign access based on role and department using the principle of least privilege.
2. Ensure multi-factor authentication (MFA) is enabled where available.
3. Keep a regularly updated access control list (ACL).
4. Onboard or remove users promptly based on HR notifications.

4.4 Secure Communication Guidelines

- Do not share sensitive information outside authorized channels.
- Enforce strong password policies and regular password changes.
- Prohibit sharing of login credentials.
- Flag suspicious links, attachments, or unexpected communications.

4.5 Role-based Permissions

1. Define permission groups (e.g., Admin, Manager, Staff, Guest).
2. Regularly review and update permissions, especially after role/department changes.
3. Restrict administrative privileges to essential personnel.

4.6 Monitoring and Maintenance

- Log and review access and usage regularly.
- Audit channel membership and permissions semi-annually.
- Apply updates, patches, and new security features promptly.
- Maintain documentation for all configuration and changes.

5. Documentation & Training

- Document all procedures, incidents, and access changes.
- Conduct mandatory user training on security and correct usage of communication channels annually.

6. Review & Revision

- Review this SOP annually or following significant incidents, platform changes, or organizational restructuring.
- Record revisions and maintain historical versions.

7. References

- IT Security Policy
- Acceptable Use Policy
- Data Privacy Guidelines

8. Appendix

- Example access request form
- Approved communication channels list