STANDARD OPERATING PROCEDURE (SOP)	
TITLE: VPN MANAGEMENT	KNUST KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Document ID:	UITS-SOP-04
Version No:	1.0
Date Authorized:	18 February 2025
Effective Date:	
Review Date:	18 February 2027
Applicable:	UITS Staff

Author(s):	**Stephen K. Osei, Papa Kwesi Quansah**
Approved by:	**Phanuel S.K. Asense**
Signature:	
Date Approved:	

1. **PURPOSE**

   This Standard Operating Procedure (SOP) outlines the steps for developing, managing, and deactivating Virtual Private Network (VPN) accounts for staff, faculty, and students at Kwame Nkrumah University of Science and Technology (KNUST). It ensures secure access to the university's network remotely while maintaining compliance with IT security policies.

2. **SCOPE**

   This SOP applies to all KNUST staff, faculty, and students who require remote access to university systems and resources through VPN. It covers:

   - VPN account creation
   - Account management (including updates and deactivation)
   - Access privileges
   - Security requirements and compliance

3. **DEFINITIONS**

   Virtual Private Network (VPN): A network that allows secure access to KNUST's internal network over an untrusted network.

   University Information Technology (UITS): The KNUST directorate responsible for managing and maintaining all IT infrastructure at KNUST.

   User: An individual or entity requiring VPN access.

4. **ROLES AND RESPONSIBILITIES**

   UITS: Oversees VPN account creation, modification, and deactivation.

   Users: Adhere to VPN usage policies and report any security issues.

   Network Administrator: Oversees VPN configuration, security settings, and user management.

5. PROCEDURES

The following are the procedures for creating, managing, and deactivating Virtual Private Network (VPN) access for users at KNUST:

5.1 VPN Account Request

5.1.1 Eligibility:

Eligibility of VPN access is based on the user's specific needs (e.g., remote work, research, or accessing campus resources).

5.1.2 Submission:

A formal request is submitted by the users via the IT Services Helpdesk (email or service portal). The request shall include:

- Name
- University ID
- Department
- Reason(s) for VPN access
- Duration of VPN access (if applicable)

5.1.3 Approval:

The VPN access request is reviewed and approved by authorized, designated staff of UITS.

5.2 VPN Account Creation

5.2.1 Account Setup:

Network administrator creates the VPN account using the user's KNUST email address and university ID.

A unique username and password credential is generated and securely sent to user via email.

5.2.2 VPN Software Installation:

Users are provided with instructions on downloading, installing, and configuring the VPN client (e.g., Cisco AnyConnect, OpenVPN).

IT Support Services offer support for installation if needed.

5.2.3 Security Requirements:

Users are required to change the default VPN password on their first login.

Two-factor authentication (2FA) shall be enforced for secure access.

5.3. Account Management

5.3.1 Account Monitoring:

The Network Administrator monitors VPN usage logs to detect any abnormal or unauthorized access.

5.3.2 Account Updates:

Users request account updates (e.g., password resets, access duration extension) by submitting a ticket to the IT Services Helpdesk.

5.3.3 Account Suspension:

Accounts are suspended automatically if inactive for 90 days.

Suspended accounts can be reactivated on user request after security verification.

5.4. VPN Account Deactivation

5.4.1 Termination:

VPN accounts are deactivated on the termination of employment, graduation, or when VPN access is no longer required.

Departments must notify UITS of staff changes for timely deactivation.

5.4.2.1.1   Audit:
UITS will conduct periodic audits of active VPN accounts to ensure only authorized personnel have access.

6. Security and Compliance

6.1.1 Usage Policy

Users must adhere to KNUST's IT usage policies while using VPN access.

Misuse of VPN accounts will result in suspension or termination of account.

6.1.2 Confidentiality:

Users are prohibited from disclosing VPN login credentials to others. A breach will result in account deactivation and/or disciplinary action.

6.1.3 Reporting

Users must report any suspicious activity or unauthorized access to the IT Services Helpdesk immediately.

7. Technical Support

Users should contact the IT Services Helpdesk for assistance with VPN access, installation, or troubleshooting.

8 Review and Updates

This SOP will be reviewed as needed based on changes in VPN technology, security policies, or organizational needs.

STANDARD OPERATING PROCEDURE (SOP)	
TITLE: VPN MANAGEMENT	

Document History	
Version	**Summary of Changes**
1.0	N/A First issue