Purpose

This Standard Operating Procedure (SOP) outlines the protocols and procedures for IT infrastructure and operations at the corporate office to ensure system reliability, data security, and efficient service delivery

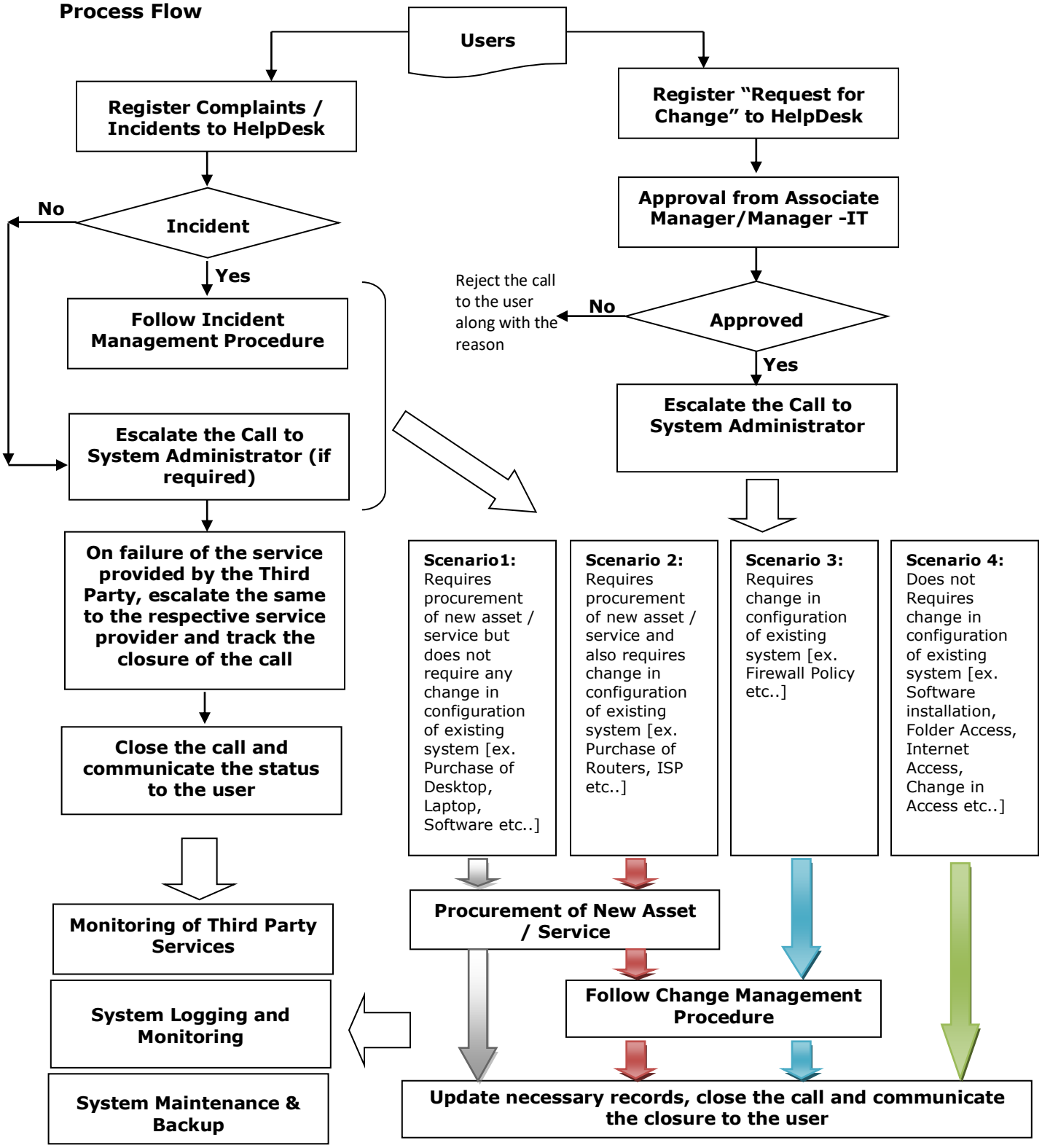
Scope
This SOP applies to all IT infrastructure and operations personnel, including system administrators, network engineers, helpdesk staff, and third-party service providers working within or supporting the corporate office IT infrastructure.

Priority Matrix:

CRITICAL	Critical tickets may prevent a customer from working or cause other devastating consequences. These tickets are often worked first or passed to a senior team member.
HIGH	High priority tickets may affect multiple staff members, customers, or departments.
MEDIUM	Medium priority tickets may affect a limited number of departments or customers. Customers may be able to continue work by applying a workaround.
NORMAL	Normal priority tickets affect only one or two customers and may present an inconvenience, but do not impede work.

- Respond to incidents based on the following SLA:
  - Critical: 1-hour response, 4-hour resolution.
  - High: 4-hour response, 8-hour resolution.
  - Medium: 8-hour response, 24-hour resolution.
  - Normal: 24-hour response, 3-business-day resolution.

Process Flow



User Registers "Compliant" or "Incidents"

a. "Incidents" will be handled as defined in the document "Incident Management Procedure"
b. Helpdesk members to check whether the complaint is pertaining to the service offered by the third party supplier and the same cannot be resolved in-house. On such occasion the help desk member shall register the complaint with the third party service provider and shall track the same with the supplier till the same is closed
c. Helpdesk members escalate the call to the system administrator if he/she is not aware of the solution and / or the solution for the compliant is unknown and / or the access provided will not be sufficient to close the compliant. System administrator will analyze the compliant for suitable solution and document the same for further reference.
d. IT SLA starts after the approval of the manager it could be of Oral/Email/Ticket approval.
e. Helpdesk member resolve the compliant only if the solution is known and also the solution doesn't require any additional privilege
f. Section 3.3 should be followed if the closure of the compliant requires procurement of any new services and / or should follow section 3.4 if it requires any change in the configuration of the current system
g. Users should be communicated about the closure of the call

User Registers "Request For Change"

a. "Request for change" should be approved by the respective Senior Managers or above [For printer & folder access the approval can be obtained from the respective managers]
b. If the request is not approved by the approving authority, the same is reverted back to the users with the reason for non-approval
c. The helpdesk member escalates the request to the Associate Manager or Manager IT if the same cannot be completed with the privilege held by the helpdesk member
d. If the request requires
h. Section 3.3 should be followed if the closure of the request requires procurement of any new services and / or should follow section 3.4 if it requires any change in the configuration of the current system
e. Helpdesk member / System administrator should update the Access Control list in case of any update in the access levels
f. Users should be communicated about the closure of the call

Procurement of New Services / Assets

a. Based on the requirement raised, the IT – Manager Shortlists two or more products and / or supplier for final decision

b. The following criteria should be considered while short listing the product and / or vendor

    a. Years of experience of the vendor / supplier in the relevant areas
    b. Reputation of the supplier in the market
    c. Supplier size
    d. Delivery time

e. Geographical Location
f. Price
g. Value added services offered by the supplier (if any)
h. Compatibility with the current environment
i. The highest classification level of information processed, and appropriate controls required ensuring the availability, integrity and confidentiality of the same
j. Validations for User Input and Output data
k. Fall back requirements / Back up
l. Access restrictions within the system
m. Reliability of the Information system
n. In case if it is to be purchased / outsourced, the level of support required from the third party, the list of requirements that are to be addressed in the agreement / contract
o. Cost of operating the controls

c. One product and / or supplier is finalized in consent with the respective Senior Manager / Operations Head.

d. On approval of the same, purchase order is raised to the supplier detailing the requirements

e. The new system is tested in line with the requirements stipulated in the Purchase order before being deployed in the current setup. In case of any deviation the same is communicated to the supplier and necessary action is taken. Any new systems should be named in line with the "Equipment Naming Convention"

f. In case of procurement of service, the Service Level Agreement should adequately cover all the clauses defined in "Outsourcing and Supply Policy"

Networking

VLANs

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. LAN port VLAN membership is assigned manually on an port-by-port basis.

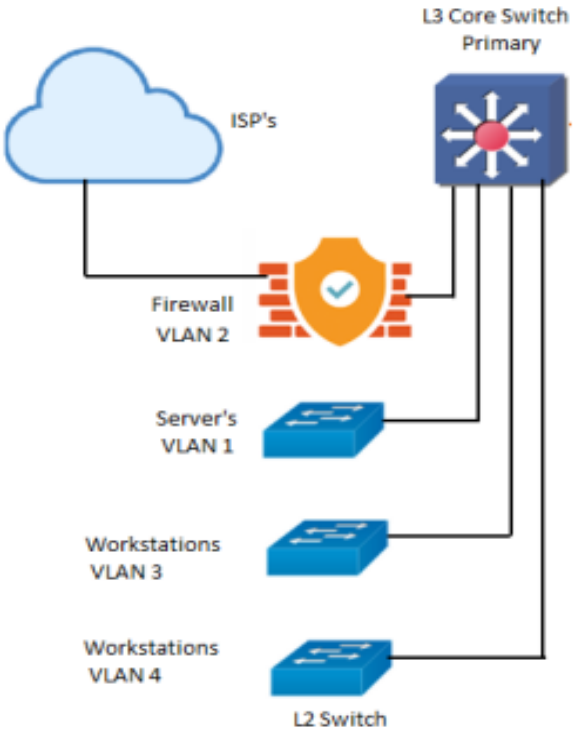
The Effect of VLANs

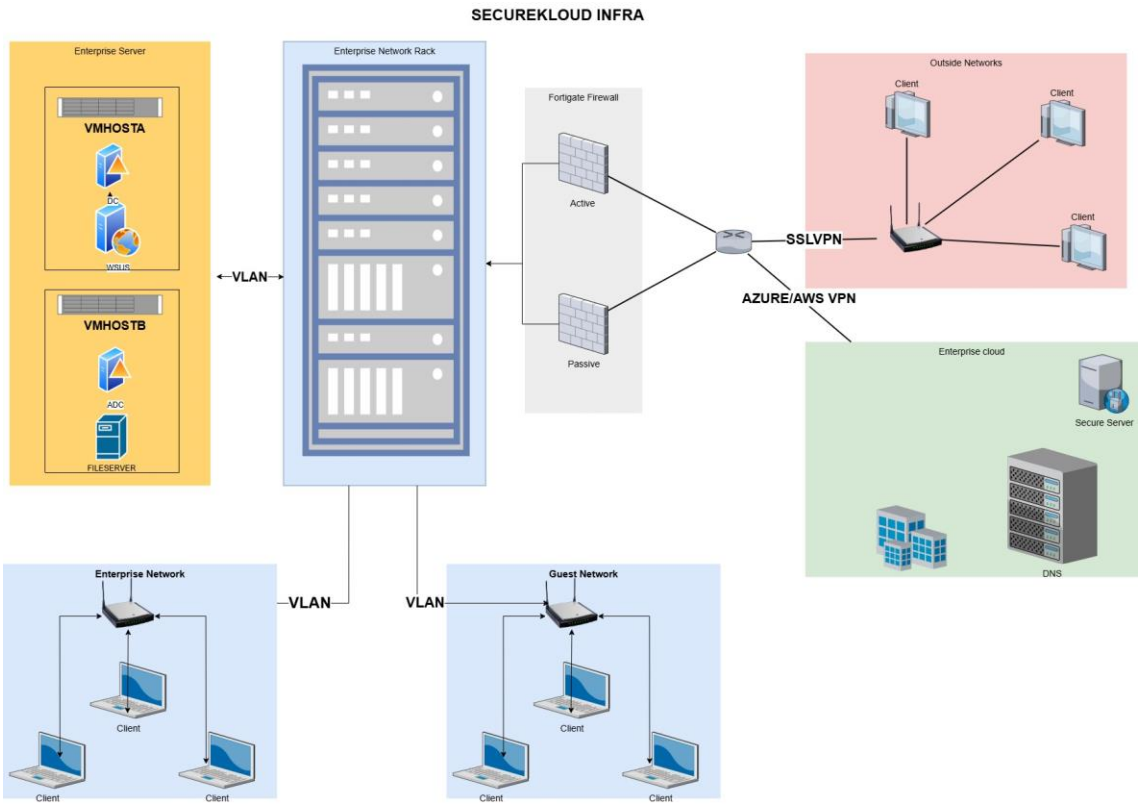
Configuring a switch for multiple VLANs reduces the size of each broadcast domain. Therefore, the amount of overhead traffic is lower which reduces bandwidth competition with data traffic. Stated another way, a node in a particular VLAN has less broadcast traffic with which to contend. Since switch

forwarding behaviour is based on MAC addresses stored in the source address table, the following rules apply:

- For known unicast destinations, the switch will forward the frame to the destination port only.
- For unknown unicast destinations, the switch will forward the frame to all active ports except the originating port. This is called flooding.
- For multicast and broadcast destinations, the switch will forward the frame to all active ports except the originating port.

SecureKloud VLAN Design





Change Control Procedure

Change Initiation

a. Helpdesk member / System administrator initiates the change request using "Change Request Form" to the corresponding Manager - IT for approval

b. The type of change shall include
   a. Hardware – Any changes to the hardware components of the IT Resources of SecureKloud
   b. Software – Any changes to the Operating systems, updates, patches etc…
   c. Databases – Any changes to the database versions, updates etc.…
   d. Network – Any change in the configuration of LAN equipment's which includes change in configuration of the firewall, switches, routers etc...

e. Facilities – UPS, Electrical etc.…

Assess and authorize the change requested

a. Manager – IT reviews the request to identify any implications involved

b. During this review the Manager – IT should consider the following

    a. Impact on security
    b. Necessity for purchasing any new information processing facility (Based on the capacity/features of the present environment)
    c. Availability of any other alternative that is comparatively more effective
    d. Change in the BCP procedures
    e. Downtime required

c. Manager – IT should seek the help of the CISO and / or Human Resource & Admin team wherever appropriate

d. Manager – IT authorizes the implementation of the change requested. If required the Manager – IT also seeks the approval of CEO / vice President for implementation of the change requested

Testing and Implementation of Changes

a. During this phase testing shall be carried out to ensure that the change doesn't impede the productivity/security of the requested department and also any other department. The test results should be documented. If the test fails either the change request should be cancelled, or the necessary steps shall be taken to ensure that the change does not impede the security/productivity. The action taken should also be documented. Wherever possible, the testing activities should be separated from the normal operations. Back up should be ensured before testing

b. Once the test results are satisfactory, the IT Tech team should take necessary steps to implement the same. Before implementation the following should be ensured

    a. How the change will be made, who will make the same
    b. Fall back procedures (if any) if the change fails
    c. Personnel to communicate about the change
    d. Disaster recovery consideration (If the change alters the current disaster recovery process, then the same should be identified)
    e. Back up of the current change

c. The plan will be executed and once the change is successful the corresponding asset inventory shall be updated (if required). If the change alters the current disaster recovery process, then the same should be updated and tested. The closure of the request should be approved once again by the Manager – IT

d. Change logs should be maintained

e. After the implementation of the changes, the same should be monitored to ensure its effectiveness

System Logging and Monitoring

Wherever technically feasible, the log should be enabled for all critical systems (ex. Firewall, Antivirus, Domain Controller). The logs should be reviewed on a periodic basis. In case of any incident identified during the log review, the same should follow "Incident Management Procedure"

System Backup & Maintenance

The critical data that are to be backed up should be identified with the help of the respective project managers; the list of backup task is maintained in the "Backup Chart" and the same is reviewed on periodic basis.

System Administrator should take the backup of the configuration on a periodic basis as defined in the "Backup Chart".

The logs of the backup should be maintained.

4. Revision History

Sl. No	Details of Revision	Rev. No.	Date	Prepared by	Approved By
1	*Procedure has been Integrated for ISO*	*01*	*16 jun 2024*	*Balaji.S Associate Manager –IT*	*Murali Krishnan.R Director-Operation*
2	*Changes in the VLAN network*	*02*	*16 jun 2024*	*Balaji .S Associate Manager –IT*	*Murali Krishnan.R Director-Operation*