**Management IP Request Form – Switch / Router**

|  |  |
| --- | --- |
| **Section 1. Requestor Information ( NAME IN BLOCK LETTERS ONLY )** | |
| **College or Department** | |
| **Engineer Full Name :** | |
| **Mobile:** | **Email :** |
| **Tel: Extension:** | **ITSM NO / CHANGE NO :** |
| **Date :** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Section 2.0 Switch / Router IP Address Request details** | | |  | |
| **Device Name – IP requested** | **Serial No** | **Device Model** | | **Device Type** |
|  |  |  | | Layer 2 **🞏** Layer 3 **🞏** |
| **Device Location (Complete Detail with Room no )** | | **Installation :New 🞏**  **: Maintenance 🞏** | | |

|  |  |
| --- | --- |
| **Section 2.1 Reason for Switch / Router IP Address Request in detail.** |  |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Affair Department Internet use only** | | |  |
| **IP Address** | **Vlan Info** | **Remarks** | |
|  |  |  | |

🞏 **I agree with terms and conditions stated at the back of this request form.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Internal use – Deanship of Information Technology – Manager / Vice Dean Approval** | | |  |
| **🞏 Approval**  **🞏 Reject**  **🞏 request info** | **Name** | **Signature** | |
|  |  | |

**NBU Switch / Router Management Policy**

***Every Switch / Management must meet the following configuration standards:***

The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device’s support organization.

* The following services or features must be disabled:
  + IP directed broadcasts
  + Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
  + TCP small services
  + UDP small services
  + All source routing and switching
  + All web services running on router
  + Telnet, FTP, and HTTP services
  + Auto-configuration
* The following services should be disabled unless a business justification is provided:
  + Discovery protocols
  + Dynamic trunking
  + Scripting environments, such as the TCL shell
* The following services must be configured:
  + Password-encryption
  + NTP configured to a corporate standard source
* Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
* Access control lists for transiting the device are to be added as business needs arise.
* The router must be included in the corporate enterprise management system with a designated point of contact.
* Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH, version 2 is the preferred management protocol.
* The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
  + IP access list accounting
  + Device logging
  + Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
  + Router console and modem access must be restricted by additional security controls.

**🞏 I agree with the terms and conditions stated in the request form and assure I have configured the device as per above stated policies before adding it into the NBU Networks.**

|  |  |  |
| --- | --- | --- |
| **Internal use – Deanship of Information Technology – Engineer** | |  |
| **Device Installation Date** |  | |
| **Signature** |  | |