Network Security Policy defines to protect Network, Information and Users.

PERN Network Security Policy

Pakistan Education & Research Network (PERN)

Version 1.0
Released June 01, 2016

1 GENERAL

Pakistan Education and Research Network (PERN) is a part of the overall vision and objectives of IT Action Plan of Government of Pakistan which was launched by the then Minister of Science & Technology. At the time of its inception, the project was jointly financed by the Ministry of Science & Technology, Government of Pakistan and PTCL (Pakistan Telecommunication Company Limited) Research & Development Funds. The network was designed by PTCL and handed over to NTC (National Telecommunication Corporation) for operations and maintenance, however it was managed by Higher Education Commission of Pakistan.

PERN focuses on collaborative research, knowledge sharing, resource sharing and distance learning by connecting people through the use of intranet and internet resources. It offers true packet switched network which is required for research and collaboration in areas like VoIP, grid computing, high energy physics, telemedicine, research related video and image exchange, enterprise level video conferencing.

PERN is a highly resilient network and the availability is ensured through a dedicated NOC which provides network operations and services on 24x7x365 basis. PERN provides special services like dedicated R&E link, 1Gbps intranet connectivity to each university/ institute, MPLS Layer3 VPN, MPLS Layer2 VPN (VLL-PWE3), VPLS, IPv4 Multicast, IPv6 Multicast, Transit AS and also ordinary services like Internet, IPv4, IPv6, Reverse DNS, Network Monitoring Services etc.

2 BACKGROUND

The project is aimed towards establishing an integral part of the overall education system of the country and is designed to interlink all public/ private sector higher education institutes (HEIs) registered with Higher Education Commission, Pakistan and other organizations/ institutes having relevance to education and research. The interconnectivity of all these organizations/ institutes will empower its users in establishing integrated data banks, collaboration for research and development, and uplifting the overall standard of teaching, learning, and research across the country as per the international norms.

Initially, the network was comprised of a backbone network connecting main hub locations in Islamabad, Lahore and Karachi. From these main hub, radial spur circuits were extended to numerous higher education institutes throughout the country. However in 2006, second phase of the project was launched by Higher Education Commission as “PERN 2” with an aim to transform the network as per international practices; whereby the network is designed, developed, operated, maintained, and managed by the partner institutions. For this, the PERN2 was designed to establish PoPs (Point of Presence) within the selected higher education institutions across the country and other institutions in vicinity are served through these PoPs in radial spurs. Moreover, in metro cities and per the needs, the network comprise of more than one PoP connected through fiber ring.

PERN2 at present comprised of three (03) Core Regional Access [cRA-PoPs] and five (05) Sub Regional Access [sRA-PoPs] interconnected through more than 6,200 Km of dark-fiber currently providing a core capacity of 10Gbps through DWDM transmission network. In metro cities, there are seven (07) Local Access [LA-PoPs] which are interconnected through more than 500 Km of metro fiber rings providing a capacity of 10Gbps through metro Ethernet technology. However, eight (08) Aggregation [A-PoPs] are established through more than 400 Km of dark-fiber providing a capacity of 1Gbps primarily through SDH transmission network.

3 DEFINITIONS

3.1 **PERN** is the acronym of the **Pakistan Education & Research Network**. The revolutionary Pakistan Education & Research Network (PERN) is a nationwide educational communicational network connecting premier education and research institutes; and providing high-speed R&E, intranet as well as internet bandwidth across the country and to international networks.

3.2 **NRENs** are National Research & Education Networks of countries around the world, e.g. MyREN (Malaysia), KOREN (Korea), UKERNA (UK), AARNET (Australia), Internet2 (USA), etc.

3.3 **PERN Principal** is referred as the Higher Education Commission of Pakistan being the custodian of PERN.

3.4 **PERN services** are all those network and application services available to partner organizations on PERN infrastructure.

3.5 **PERN resources** are all those tangible and intangible assets, hardware equipment and software tools, as well as human workforce, involved in operating the PERN infrastructure and PERN services.

3.6 **Consortium of NRENs** is a network of NRENs interconnected to form a large community for collaboration for education and research, e.g. TEIN (TransEurasia Information Network), GEANT (Pan-European Advanced Network), etc.

3.7 **Partner Organization** refers to all organizations getting R&E services from PERN and contributing towards sustainability of this network.

3.8 **HEIs** refer to higher education institutions both public and private sector universities, centers of excellence, affiliated colleges, degree/ postgraduate colleges, etc.

3.9 **Last Mile Connection** is a connectivity between organization and nearest circuit termination point to take the traffic further to PERN aggregation points or host organization.

3.10 **International traffic** is the traffic between the PERN and any other international Public network (Internet).

3.11 **R&E traffic** of the NRENs is the traffic between the PERN and any other NRENs or network

of NRENs of the world.

3.12 **Packaged Digital Resources** are a set of services provided by PERN to its users for example digital library, Video conferencing etc.

3.13 **PERN Subscription Plan** are a set of services provided by PERN to the users.

4 SCOPE

Without a security policy, the availability of the PERN2 network can be compromised. This policy begins with understanding the risks, assessing the risk to the network and mechanism to respond on any risk. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy as needed and adapts to lessons learned.

5 POLICY

This document is divided into three phases: preparation, prevention, and response;

5.1 Preparation

Users' roles and responsibilities with regard to security are outlined in the Acceptable Use Policy and Information Security Policy.

5.1.1 Administrator Acceptable Use Statement - The head of IT for any HEI is hereby responsible for developing and maintaining an administrator acceptable use statement to explain the procedures for user account administration, policy enforcement, and privilege review. The Director of Operations or any head of IT for any HEI will ensure that administrator requirements listed in the acceptable use policy are reflected in training plans and performance evaluations. Specific policies concerning network security & incident related Security Policy respectively.

5.1.2 Security Team - The head of IT for HEI will lead a security team comprised of the Director PERN, Deputy Director/Assistant System/Network or Network/Security Engineer/ Specialist The security team has three areas of responsibility: policy development, practice, and response. Policy development is focused on establishing and reviewing security policies for the institution on bi-annual basis, to include the risk analysis. Practice is the stage during which the security team conducts the risk analysis; the approval of security change requests; reviews security bulletins and alerts. The head of IT for HEI will lead a security team comprised of the Director PERN, Deputy Director/Assistant System/Network or Network/Security Engineer/ Specialist The security team has three areas of responsibility: policy development, practice, and response. Policy development is focused on establishing and reviewing security policies for the institution on bi-annual basis, to include the risk analysis. Practice is the stage during which the security team conducts the risk analysis; the

approval of security change requests; reviews security bulletins and alerts.

5.2 **Prevention**

Prevention is broken down into two parts: approving security changes and monitoring security of the network

5.2.1 Approving Security Changes - Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. The Deputy Director System/Network the Information Security Specialist are responsible for proposing security changes to the security team for approval. Examples include, but are not limited to, the following:

- Any change to the Router/firewall configuration pertaining to Security.
- Any change to the access control lists (ACL).
- Any change to Simple Network Management Protocol (SNMP) configuration.
- Other Security appliances Configuration as well.

Any member of the security team can deny a change request that is considered a security change until it has been approved by the security team. In emergency situations, the Network Engineer PERN2 and the Information Security Specialist can authorize security changes providing such changes are immediately brought to the attention of the security team.

5.2.2 Monitoring Security of the Network - Security monitoring is similar to network monitoring, except it focuses on detecting changes in the network that indicate a security violation. The starting point for security monitoring is determining what a violation is. In conducting a Risk Analysis, the security team identifies the level of monitoring required based on the threat to the system. In Approving Security Changes, the security team identifies specific threats to the network. By looking at both of these parameters, the security team will be able to develop a clear picture of what needs to be monitored and how often. Low-risk equipment will be monitored on a weekly basis, medium-risk equipment on a daily basis, and high-risk equipment on an hourly basis. Following points are mandatory to enable in Campus Network:

a. It is important to enable Security logs on all the Router, Servers, and Firewall & IPs. The Log should be kept for 3 month period of time.

b. For Campus network it is important to enable Firewall & IPS on perimeter/Core.

c. For Campus network it is important to have centralize logs collected in Single Dashboard like SIEM. The logs should be collected from all Server like: Active Directory, Proxy, Databases, webservers & Network appliances like: Router,

Switches, and Firewall & Intrusion Prevention System.

d. Log monitoring can be perform on daily basis & sever incidents may be logged.

5.3 **Response**

Response is broken into three parts: security violations, restoration, and review

5.3.1 Security Violation - When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having guidelines in place to make these decisions ahead of time makes responding to an intrusion much more manageable. The security team is responsible for developing a notification system that is available 24 hours a day, 7 days a week. Additionally, the security team is responsible for defining the level of authority given to the Deputy Director Network/System, Network Engineer or Security Specialist to make changes and in what order the changes should be made. Possible corrective actions are:

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.
- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting the violated systems or the source of the violation.
- Contacting the police, or other governmental agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel.

To determine the extent of the violations, the security team will do the following

- Record events by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.
- Limit further compromises by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.
- Backup compromised systems to aid in a detailed analysis of the damage and method of attack.
- Look for signs of compromise. Often when a system is compromised, there are other systems or accounts involved.
- Maintain and review security device log files and networking monitoring log files, as they often provide clues to methods of attack

6 REVISION IN POLICY

This policy shall be regularly reviewed for possible revision, if deem necessary, in any eventuality in PERN infrastructure, resources and services. Amended texts shall be approved by the PERN Principal and shall be made publically available.