Azure Power®

AZURE POWER INDIA PVT. LTD.

POLICY

COMMUNICATIONS SECURITY

DOC. NO: APIPL-IS-POL-CS

Rev. Number: 00 **Date: 28-05-2019**

Document Summary

Document Reference ID	APIPL-IS-POL-CS
Version Number	1.0
Document Type	Policy
Author	Sr Executive - IT AMIT SUNDRIYAL
Reviewed By	DGM-IT
Approved By	Head IT
Release Date	28-May-2019

Revision History

Version	Date	Author	Significant Changes

Contents

1. Introduction

1.1 Intent

Communication Security Policy is an essential prerequisite to sound Information Security Management. This policy formulates the controls for the security of key areas in the day to day Information Technology (IT) communications management of Azure Power (India) Private Limited (Henceforth referred to as APIPL). These controls provide protection against vulnerabilities and attacks within APIPL's IT environment.

The purpose of this policy is:

- To protect the integrity and availability of APIPL's communication services
- To ensure the protection of information in APIPL's networks and supporting information processing facilities

1.2 Scope

This policy applies to all individuals who access, use or control APIPL owned resources. This includes but is not limited to APIPL's employees, contractors, consultants, and other workers including all personnel affiliated to external organizations with access to the APIPL's network.

The term employee(s), its synonyms (staff, personnel etc.) and vice versa hereafter encompasses the scope defined in the paragraph above.

1.3 Roles

S.No.	Key Practice	Responsibility
1.	Network Security	Head, IT Department/CISO
2..	Confidentiality or Non-Disclosure Agreements	Legal Department/CISO

3.	Review of Confidentiality or Non-Disclosure Agreements Requirements	Head of Engaging Department/ Business Unit and Chief Information Security Officer (CISO)

2. Policy

2.1 Communications Security

2.1.1 Network Security Management

2.1.1.1 Network Controls

- General
  - ➢ Each user shall be allocated a separate login account.
  - ➢ Separate login account shall be used for operating at different privilege levels.
  - ➢ Network Devices and Network Security Devices shall have at least two administrators.
  - ➢ Hostname shall not reveal make / model of the device.
  - ➢ Encrypted channel shall be used for remote administration.
  - ➢ Services not needed for conduct of business shall be disabled.
  - ➢ *Change Management Process (APIPL-IS-PRO-C&PM)* shall be followed for any addition / deletion / modification of the devices.
  - ➢ Configuration of the device shall be erased before disposal.

- Firewall
  - ➢ Change management process shall be followed for any change in the rule base.
  - ➢ Use of 'Any' in permit statements in the rule base shall be avoided.
  - ➢ 'Deny all unless explicitly allowed' policy shall be used.

- ➢ Rules shall be properly commented.
- ➢ All traffic destined to the firewall IP address (except for VPN or management purpose) shall be dropped and logged.
- ➢ Anti-Spoofing shall be enabled on all interfaces.
- ➢ Attacks such as 'Denial of Service, Ping of Death, Source-routed Packets', etc. shall be blocked by using suitable counter measures.
- ➢ Firewall shall be deployed in High Availability mode.

- Router Configuration
  - ➢ Authentication shall be used for dynamic routing protocols.
  - ➢ Ingress and Egress filtering shall be configured.
  - ➢ Unused address space shall be routed to null interface.
  - ➢ Anti-spoofing shall be enabled on all interfaces.
- Operating Systems Upgrade
  - ➢ Latest stable software version shall be selected.
  - ➢ Minimum system requirements for the upgrade shall be ascertained.
  - ➢ Backup of the current operating system and the running configuration shall be taken prior to upgrade.
- Simple Network Management Protocol
  - ➢ Enable SNMP if required.
  - ➢ SNMPv3 or higher (if/ when available) should be used.
  - ➢ Default community string (for example: 'public') shall not be used.
  - ➢ Community string security shall be treated at par with Administrator account password.
  - ➢ Community string shall be set for read-only mode.
  - ➢ SNMP access shall be permitted from specific IP addresses of trusted networks.

- Same or similar community strings shall not be used across devices.

- Banner Message
  - Warning message shall be displayed before login as a caution for all network devices.
  - A sample banner message follows :

Azure Power Pvt Ltd

IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION.

This system is restricted to authorized users. If you are unauthorized to login kindly logoff now.

Click OK to indicate your acceptance of this information

2.1.1.2 Security of Network Devices

- Security Mechanisms, service levels and management requirements of all network services shall be identified and included in network service agreements, whether these services are provided in-house or outsourced.

2.1.1.3 Segregation in Networks

- Groups of information services, users, information systems shall be segregated on network.

2.1.2 Information Transfer

2.1.2.1 Information Transfer Policies and Procedures

- Formal transfer policies and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. *Refer: ISMS Information Transfer Policy (APIPL-IS-POL-IT)*.

2.1.2.2 Agreements on Information Transfer

- Agreements shall address the secure transfer of business information between APIPL and external parties.

2.1.2.3 Electronic Messaging

- There shall be only one official e-mail system in the organization.
- All employees shall be provided with e-mail id and shall use it for official correspondence within and outside the organization.
- Individual user shall be responsible for all e-mails sent from his/her account.
- E-mail account password shall be resets for all the employee separated from APIPL. Further, employee email account shall be deleted within 3 months of separation.
- The owner of the e-mail account shall be held responsible, if his/ her account has been used to compromise the organization, e.g. sending defamatory e-mail, use of harassment, unauthorized purchasing etc. and any violations shall be cause for disciplinary action in accordance with the HR Code of conduct Policy. *Refer: ISMS Acceptable Usage Policy (APIPL-IS-POL-AU)*
- The server logs and the electronic 'paper trails' shall be considered proof for deciding misuse of e-mail.
- The user shall not configure any external server mailboxes on his/ her workstation and shall be completely responsible for the security hazard posed in case the external mail server is not secure.
- The mails being sent outside the organization shall carry a standard 'Disclaimer'.
- APIPL encourages the use of electronic mail and does not intend to inspect or monitor electronic mail routinely or to be the arbiter of its contents. Nonetheless, the electronic mail and data stored on the APIPL mail network of computers may be accessed by the Company for the following purposes:
  - Troubleshooting hardware and software problems.
  - Preventing unauthorized access and system misuse.
  - Retrieving business related information from any mail account.
  - Complying with legal requests for information.
  - Re-routing or disposing of undeliverable mail.

- E-mail Use: Policy for Users:
    - Only the e-mail account provided by APIPL shall be used for official communication.
    - E-mail password shall not be shared even for official purpose.
    - User shall not attempt any unauthorized use of e-mail services, such as:
        - Distribution of messages anonymously.
        - Misusing other user's e-mail address.
        - Using a false identity.
        - Sending messages to harass or intimidate others.
    - Password used for online forms/services/ registrations /subscriptions shall not be the same as the password of official e-mail account (domain ID).
    - Refer: ISMS *Acceptable Usage Policy (APIPL-IS-POL-AU)* and ISMS *Password Management Policy (APIPL-IS-POL-PM)*

2.1.2.4 Confidentiality or Non- Disclosure Agreements

- Requirements for confidentiality or non-disclosure agreements reflecting APIPL's needs for the protection of information shall be identified and documented by the Legal Department.
- The same shall be reviewed on a periodic basis by the Chief Information Security Officer (CISO).

3. Compliance

All members of staff and users of APIPL's owned resources must comply with this policy/ procedure. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, in keeping with HR *Code of Conduct Policy.*

The following processes are utilized to enforce compliance with this policy/ procedure and supporting standards:-

- Monitoring: the company employs appropriate technology solutions to monitor policy/ procedure compliance.

- Self-Assessment: Managers and Department Heads are required to conduct self-assessment within their areas of control to verify compliance to this policy/ procedure.
- Security Audits: Internal Audit may assess the implementation of and compliance with this policy/ procedure as part of its audit program.

3.1 Special Circumstances and Exceptions

All exceptions to this policy/ procedure will require a waiver explicitly approved by APIPL's Chief Information Security Officer (CISO).