IT POLICY

National Power Parks Management Company

Ministry of Energy, Power Division

Government of Pakistan

IT POLICY May 2018	Issuing Officer Company Secretary Target Audience All employees and users. Approving Authority Board of Directors Issuing Date May 22, 2018 Revision Initial Issue Copy Rights National Power Parks Management Company (Pvt.) Ltd.

National Power Parks Management Company (Pvt) Ltd.

1. POLICY STATEMENT

National Power Park Management Company (Pvt.) Limited (the "Company") acknowledges that Information Technology (IT) has become a key business driver in organizations. However, wide spread use of IT systems also poses dangers to the integrity of a business. Therefore, it has increasingly become important to set out clear rules and guidelines for properly managing the use of IT systems and for protection against internal and external threats.

2. OBJECTIVES

2.1 To ensure effective usage of IT Systems and Resources for business needs;

2.2 To protect IT Systems and Resources from external and internal threats;

2.3 To ensure integrity of data and information;

2.4 To establish control mechanisms to protect IT Systems and Resources against theft, abuse and other forms of harm or loss; and,

2.5 To provide direction to the employees as to what constitute appropriate use, how to do incident reporting and how to ensure business continuity.

3. SCOPE

3.1 The policy is applicable to all employees of the Company.

3.2 This policy also covers those who are using Company's IT Systems and Resources directly or indirectly.

3.3 This policy encompasses all IT Systems and Resources of the Company.

4. GUIDING PRINCIPLES

4.1 Availability

Use of IT Systems and Resources must ensure availability and accessibility of information and data at all times.

4.2 Security

Use of IT Systems and Resources must maintain confidentiality - Information and data must not be made available or disclosed to unauthorized individuals, entities or processes.

4.3 Integrity

IT Systems and Resources must be able to ensure that data must not be altered or destroyed in an unauthorized manner, and accuracy and consistency must be preserved regardless of changes.

4.4 Multidisciplinary

IT Systems and Resources must be able to support Company's goals and cater for its multi-disciplinary requirements besides adding value to the Company.

5. PROCEDURAL GUIDELINES

5.1 Acceptable Use of Company's IT Systems and Resources

5.1.1 Unless otherwise specified in this policy or any other policy of the Company, use of Company's IT Systems and Resources is strictly restricted to purposes

National Power Park Management Company (Pvt.) Ltd.

related to official business of the Company.

5.1.2 Incidental personal use of Company's IT systems and resources must adhere to all applicable Company policies and procedures and under no circumstances may involve violations of the law, interfere with the fulfillment of Company's business needs or any other employee's responsibilities.

5.1.3 Only eligible users, as may be authenticated by GM (Admin/HR), shall be entitled to use Company's IT Systems and Resources.

5.1.4 The IT Systems and Resources include, but not limited to, provision and use of laptops, desktops, printers, servers, Local Area Network (LAN), Wide Area Network (WAN), portable media devices, internet bandwidth, system and application software and physical environment.

5.1.5 The users of Company's IT Systems and Resources are prohibited from engaging in any activity that is illegal under local, provincial, federal or international law or in violation of Company's policies.

5.2 Un-acceptable Use of Company's IT Systems and Resources

5.2.1 Obtaining configuration information about a network or system for which the user does not have authorization;

5.2.2 Engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network;

5.2.3 Circumventing user authentication or accessing date, accounts, or systems that the user is not expressly authorized to access;

5.2.4 Interfering with or denying service to another user on the network or using Company's facilities or networks to interfere or deny service to persons outside the Company;

5.2.5 Users may not use Company's IT Systems and Resources to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations;

5.2.6 Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.);

5.2.7 Changing another user's password, access, or authentications;

5.2.8 Using someone else's credentials without approval of such user;

5.2.9 Using Company's IT Systems and Resources to actively engage in displaying, procuring, or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity;

5.2.10 Sending unsolicited messages or other advertising material, to individuals who did not specifically request such material form official IT Systems and Resources;

5.2.11 Engaging in harassment via electronic communications whether through language, frequency, or size of messages;

5.2.12 Masquerading as someone else by using their email or internet address or electronic signature; and,

5.2.13 The unacceptable usage as mentioned above are by no means exhaustive, but attempts to provide a framework of activities that fall into

National Power Parks Management Company (Pvt) Ltd. *

the category of unacceptable use.

5.3 Use of Emails and Internet

5.3.1 Internet

a) The Company provides its employees with internet facility to be used in performance of their official work. As such employees are expected to use internet responsibly and productively.

b) The Company's employees are discouraged from participating in discussions about the Company on internet e.g. on discussion/social media forums, chat rooms, or bulletin boards. The employees may not, at any time, discuss confidential and material information.

c) The Company's employees must not visit websites that can compromise the safety of company's network and computers, also must not perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods.

d) All sites and downloads may be monitored and/or blocked by the Company if they are deemed to be harmful and/or not productive to business.

5.3.2 Emails

a) The Company provides its employees with an electronic mail system. The primary purpose of the electronic mail system is to expedite necessary business communications between two or more individuals. As such, the use of electronic mail is for the Company's business purposes only.

b) Use of official email is a privilege and may be revoked at any time.

c) Any information included in email communications using the office email system becomes the property of the Company and subject to monitoring on approval of the Audit Committee.

d) All users of the Company's email account shall change the password of their respective email accounts after every 90 days for security reasons.

e) All electronic communications and stored information transmitted, received, or archived in the Company's information system are the property of the Company.

f) Emails sent via the Company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

g) The Company reserves the right to access all messages sent by office e-mail. There is no right to privacy when using the organizational email system.

h) The Company holds the right of privacy of material on its email system. No external organization has rights to view or modify organizational email except where explicitly mandated by law.

i) The Company's email system may not be used for sending spam.

j) The Company's email system may not be used for sending mass emails

National Power Parks Management company (Pvt) Ltd.

without the consent and guidance of IT Function (IT Team).

k) All users of the official emails must use a standardized disclaimer statement attached as **Annex-A** on all of its outgoing emails.

5.4 General Controls

5.4.1 IT Function shall maintain a log of all laptop devices by serial number, the date they were deployed, to whom they were deployed, and the return date. Proper handing / taking over procedures must be developed by the IT Department for this purpose.

5.4.2 All laptops and desktops provided to the employees and other users must be encrypted with access to the Company's IT networks via using an appropriate authentication method;

5.4.3 In case of installation rights on the laptop / desktop, Company's employee(s) must not install any unlicensed Software(s).

5.4.4 Portable IT Systems and Resources in users' custody should not be exposed to opportunistic theft;

5.4.5 It shall be the duty of users to keep the portable IT Systems and Resources safe and secure and to avoid its misuse;

5.4.6 Loss, theft or damage of IT systems and Resources in the custody of users shall be the responsibility of the user; and if the loss, theft or damage is found to be due to the user's negligence, all the expense would be the responsibility of the user on book value;

5.4.7 The user shall not be responsible for loss, theft or damage if it does not happen due to his/her negligence or happened accidentally. It will be the management's responsibility to determine whether the theft was due to user's negligence or not;

5.4.8 Any loss or theft of IT System / laptop must be immediately reported to the IT Function, so they can timely block the access of corporate IT services from the laptop.

5.4.9 Upon termination, the IT Function must ensure that IT Systems and Resources must be returned on the last day of service of employee in the Company, however, in case of termination due to disciplinary reasons, the IT Systems and Resources shall be taken back on the same business day;

5.4.10 If the IT Systems and Resources in the custody of a user are not found in a good condition or has been misplaced/damaged the book value of the same shall be deducted from the user's final settlement;

5.4.11 The Company will minimize the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software. Users are encouraged to report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately to the IT Function;

5.4.12 The Company shall put in place adequate physical access and environmental controls;

5.4.13 Third party audits may be conducted as and when required to ensure proper placement of IT security controls.

5.4.14 The Company shall insure its necessary IT Systems and Resources from an insurance company against damage, theft, loss and disaster etc., along

National Power Parks Management company (Pvt) Ltd. *

with their annual renewal.

5.5 System Controls

5.5.1 Application Account Controls

a) All accounts must use multifactor authentication if the technology is available and implemented;

b) Each account must use a password as per Company's password guidelines under this policy;

c) All unused accounts must be blocked/deleted as soon as practicable;

d) Each account must be granted the least privilege to perform required job function(s);

e) Each account must be assigned to one individual or to one service.

5.5.2 Server Controls

a) Local login access to the system must be restricted by access control list to those accounts with a documented business need to use data on the system;

b) Remote login access to the system must be restricted to those accounts with a documented business need to use data on the system remotely.

c) Accounts with access to the system will be regularly reviewed, and access will be removed when a business need no longer exists for that access;

d) Only the minimum operating system components required to carry out the business function shall be installed;

e) Security updates to the operating system and application services shall be installed expeditiously;

f) If automated notification of operating system and application updates is available, it shall be enabled;

g) A licensed anti-virus program must be installed, running, and have on-access scanning and automatic updates enabled;

h) Systems must run only the services required to perform the specific business function of the machine;

i) Systems must have session timeouts and screen locks enabled;

j) All file systems containing critical system files or protected data must require authentication and support access control;

k) All privileged access must be logged, e.g., administrator;

l) Storage media and systems must be clearly labelled with "Restricted Data" stickers.

5.5.3 Network Controls

a) System must be on an enterprise grade firewall protected network shared only with systems in the same security domain;

b) IT Function must check intrusion detection logs on regular basis

c) Network access (both for internal (LAN) and external (WAN) side) shall be restricted to the minimum necessary to perform required functions.

d) VLANs must be used to logically separate the data communication of

National Power Park Management company (Pvt) Ltd. *

Company's Departments.

5.5.4 Physical Controls

a) Systems (Servers, Storage, Security Devices, etc.) must be located in a locked room with limited access;

b) Biometric based locking system must be used to access the Server Room / Data Center and all access must be logged.

c) CCTV Monitoring System must be installed to cover the entire Datacenter / Server Room.

d) Back-up media must be physically secured from un-authorized access;

e) Systems must be provided with power protection - air conditioning, uninterruptable power supply UPS, and back-up generator;

f) Systems must be located in a room with appropriate environmental controls.

g) Server Room must have smoke detection system in order to timely alert in case of any fire incident(s). Fire suppressions equipment must also be available with server room. System storage media must be securely erased or disposed-of when system function/role changes including equipment disposal.

h) IT Function must make themselves familiar with applicable health and safety rules for working within a data center.

i) IT Function must not bring food, drink or other 'wet' items (e.g. coats and umbrellas) into or through the data center.

j) It Function should arrange for the removal of any equipment no longer required as soon as possible after decommissioning.

k) IT Function must not leave unlocked or prop open any access door to the data center.

l) It Function must not enable unauthorized persons to enter the data center. In particular, IT Function must not share his key or access codes with any other individual and nor must be accompanied by any unauthorized person.

5.5.5 Change Management

a) IT Function must establish and document change control process for system configuration;

b) System changes and patches must be evaluated and tested prior to installation in a production environment.

5.6 IT Security Incident Reporting and Disaster Recovery

5.6.1 For the purpose of this policy an "IT security incident" is any accidental or malicious act with the potential to:

a) Result in misappropriation or misuse of confidential information;

b) Significantly imperil the functionality of the IT systems or resources;

c) Provide for unauthorized access to Company information or data;

d) Allow IT systems or resources of Company to be used to launch attacks against the resources and information of other individuals or

National Power Parks Management Company (Pvt) Ltd.

organizations.

5.6.2 Users should first attempt to stop any IT security incident as it occurs by powering-down the computer or disconnecting it from the Company's IT network.

5.6.3 Users must report IT security incident to the Company's IT Function. The IT Function will help in assessing the problem and determine how to proceed.

5.6.4 Following the report users should comply with directions provided by IT Function to repair the system, restore service, and preserve evidence of the incident.

5.6.5 In case of an IT security incident, the IT Function should:

a) Respond quickly to reports from users;

b) Take immediate action to stop the incident from continuing or recurring;

c) Determine whether the incident should be handled locally or reported to the IT Security Response Team (ITSRT);

d) If the incident does not involve the loss of confidential information or have serious impacts to users or the Company, the IT Function should repair the system, restore service, and preserve evidence of the incident;

e) If the incident involves the loss of confidential information or critical data or has other potentially serious impacts, the IT Function should:

1. File an IT Security Incident Report including a description of the incident and documenting any actions taken thus far with the ITSRT;
2. The ITSRT will investigate the incident in consultation with the IT Function and develop a response plan;
3. Notify to the Admin Department that an incident has occurred and that the ITSRT has been contacted;
4. Refrain from discussing the incident with other until a response plan has been formulated.
5. Follow the ITSRT response plan to repair the system and restore service, and preserve evidence of the incident.

5.6.6 ITSRT shall comprise of Chief Internal Auditor, GM (Admin/HR) and the Company Secretary.

5.6.7 ITRST shall meet on quarterly basis to prepare disaster recovery plans and procedures to cater for the disaster events such as flash floods, building fires, hard drive meltdowns due to power fluctuations, earthquakes, terrorist attacks or acts of war etc.

5.7 Backup, Storage and Business Continuity

5.7.1 Back-up of important information, data, emails and other electronic files shall be maintained by the users and IT Function on fortnightly basis.

5.7.2 The purpose of back-ups is to restore a system to a current state (as of the date of the most recent back-up) in case of system failure, or to restore individual files inadvertently deleted or lost.

5.7.3 Back-up media is also intended to serve as a short or long-term storage of information.

National Power Parks Management Company (Pvt) Ltd. ★

5.7.4 Back-ups of email and other files should be retained for no more than five years, whereas, all other back-ups shall be retained for more than five-years;

5.7.5 The IT Function must establish, document, and follow a regular back-up schedule;

5.7.6 The ability to restore from back-up must be tested at least once a month – automated verification, user initiated, or trial restores are acceptable methods.

5.7.7 Keeping in view the critical nature of the business a Disaster Recovery sites must be maintained in order to provide uninterrupted IT Services in case of disaster at main site / datacenter.

5.7.8 Offsite backups must also be maintained by the IT Function.

5.8 End Users Support / IT Helpdesk Support.

5.8.1 IT Helpdesk should be created to provide "First Level" technical support to end users to ensure the smooth functioning of business applications and IT services.

5.8.2 The method(s) to be used to contact the help desk such as telephone number(s) and email addresses(s) must be defined and communicated to all the stakeholders / users of the systems.

5.8.3 IT help desk should coordinate with different vendors in case of any issues which cannot be solved by local IT team.

5.9 Asset Tracking / IT Inventory Management

All IT Assets (Desktop / Workstations, Laptop Printers, Copiers etc. should be tracked and documented in the Fixed Assets Register or Inventory Management System. All assets should have a unique ID number and all addition/deletion/transfer must be properly logged.

5.10 Securing data upon Asset Disposal

Asset disposal of any storage device is a special case since the asset must have any sensitive data removed prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.

2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.

3. Medium (Confidential) - The data must be erased using an approved technology / industry standard to make sure it is not readable using special hi-tech techniques.

National Power Parks Management company (Pvt) Ltd.

5.11 Packaged / Custom Built Applications Adoption Guidelines

5.11.1 The standard business process should be automated by either adopting packaged solution or a custom developed

5.11.2 customized software(s) could be developed by the IT Function of the company or outsourced to a suitable software firm.

5.12 Password Protection Guidelines

5.12.1 All user-level and system-level passwords must conform to the Password Construction Guidelines **(Annex - B-)**.

5.12.2 User must not use same passwords for their other accounts or access needs especially where system-level privileges have been granted. Password for system-level privileges must be unique.

5.12.3 All System-Level Passwords must be changed on at least quarterly basis.

5.12.4 All User-Level Passwords must be changed on at least bi-annual basis.

5.12.5 IT Function may perform occasional password cracking or guessing. If a password is guessed or cracked during such an exercise, the user will be required to change the password in conformity with the Password Construction Guidelines.

5.12.6 Passwords must not be shared with anyone or inserted into email messages or other forms of electronic communication (Telephone, Chat, etc.)

5.12.7 Users must not write down and store passwords anywhere in their offices or workplace or on a computer system or mobile device without encryption.

5.12.8 Users must not use "Remember Password" feature of applications e.g., web-browsers.

5.12.9 User must be careful about letting someone see him typing his/her password.

5.12.10 Any user suspecting that his/her password may have been compromised must report the incident and immediately change all passwords.

5.12.11 IT Function must set an account lockout threshold of 4 failed login attempts. Administrator can only reset the locked-out account.

5.12.12 Responsibility to keep password secure resides with the user.

6. GLOSSARY OF TERMS

"Users" means all employees and other users as may be allowed to use Company's IT Systems and Resources under this policy.

"IT Function" means official(s) hired and mandated with the task to handle IT related duties in the Company.

"System-Level Passwords" means passwords used at application level.

"User-Level Passwords" means passwords used at personal devices and accounts.

National Power Parks Management company (Pvt) Ltd. *

7. IMPLEMENTATION AND COMPLIANCE OF THIS POLICY

7.1 The Company's IT Function shall be primarily responsible to ensure implementation and compliance of this policy under the supervision and guidance of administration department.

7.2 The IT Function may ensure compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal audits, and feed-back.

7.3 GM (Admin/HR) shall be authorized to approve detailed procedures to give effect to various provisions under this policy.

8. NON-COMPLIANCE WITH THIS POLICY

8.1 The users are responsible for consulting, understanding, and complying with this policy.

8.2 Failure to comply with this policy by the employees may result in disciplinary action.

9. SAVINGS

This policy can be changed, modified or abrogated at any time by the Audit Committee.

National Power Parks Management company (Pvt) Ltd. ★

ANNEX-A

DISCLAIMER STATEMENT

Disclaimer: National Power Parks Management Company (Private) Limited (NPPMCL) accepts no liability for private publication of any content or statement by any of its employees or for the consequences of any action taken on the basis of such publication or statement. The information in this email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. If you have received this message in error, please notify us and delete it from your computer. NPPMCL accepts no liability for any loss or damage caused by any virus transmitted by this email.

National Power Parks Management company (Pvt) Ltd.

ANNEX-B
PASSWORD CONSTRUCTION GUIDELINES

Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters.
- Contain both upper and lower-case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123".

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

National Power Parks Management Company (Pvt) Ltd. ✦