1 Policy

1.1 Policy for Acceptable Use of Information Assets

1.1.1 General Use

- While BeyonData Solutions Pvt. Ltd.' IT Division desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of BeyonData Solutions Pvt. Ltd. Because of the need to protect BeyonData Solutions Pvt. Ltd.' network, management cannot guarantee the confidentiality of information stored on any network device belonging to BeyonData Solutions Pvt. Ltd.
- For security and network maintenance purposes, authorized individuals within BeyonData Solutions Pvt. Ltd. may monitor equipment, systems, and network traffic at any time.
- BeyonData Solutions Pvt. Ltd. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.1.2 Security and Proprietary Information

- The user interface for information contained on internet/Intranet/Extranet-related systems should be classified as Confidential, Internal or Public, as defined as per Procedure for Identification, classification, and valuation of information asset. Examples of confidential information include but are not limited to company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Email password should be changed every 60 Days.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes when the host is unattended.
- Because information contained on portable computers Is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Policy".
- Postings by employees from BeyonData Solutions Pvt. Ltd. email address to newsgroups should I contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of BeyonData Solutions Pvt. Ltd., unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

1.1.3 Unacceptable Use

The following activities are in general prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances, an employee of BeyonData Solutions Pvt. Ltd. is authorized to engage in any activity that is illegal under law while utilizing BeyonData Solutions Pvt. Ltd. Owned resources. The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by BeyonData Solutions Pvt. Ltd.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which BeyonData Solutions Pvt. Ltd. or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using BeyonData Solutions Pvt. Ltd. computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any BeyonData Solutions Pvt. Ltd. account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty. 1 security Circumventing user authentication or ity of any host, network, or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a
- User's terminal session, via any means, locally or via the Internet/Intranet/Extranet. 1
- Providing information about or lists of. BeyonData Solutions Pvt. Ltd. employees to parties outside BeyonData Solutions Pvt. Ltd.

1.1.4 Blogging

- Blogging by employees, whether using BeyonData Solutions Pvt. Ltd.' property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of BeyonData Solutions Pvt. Ltd.'

systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate BeyonData Solutions Pvt. Ltd.' policy, is not detrimental to BeyonData Solutions Pvt. Ltd.' best interests, and does not interfere with an employee's regular work duties. Blogging from BeyonData Solutions Pvt. Ltd.' systems is also subject to monitoring.

- BeyonData Solutions Pvt. Ltd.' Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Company confidential or proprietary information, trade secrets or any other material covered by Company's Confidential Information policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of BeyonData Solutions Pvt. Ltd. and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, comments when blogging or otherwise engaging in any conduct prohibited by elnfachids' with blogging. • Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, BeyonData Solutions Pvt. Ltd.' trademarks, logos and any other BeyonData Solutions Pvt. Ltd. intellectual property may also not be used in connection with any blogging activity.

1.2 Policy for Network control

1.2.1 Configuring Networks.

- The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.
- The configuration of network impacts directly on its performance and affects its stability and Information Security.
- Information Security issues to be considered when implementing policy include the following:
- Network stability shall be good enough to protect business operations.
- Adequate control over access to network shall be applied to protect the confidentiality and integrity of data.
- Adequate system response times shall be ensured.
- Configuration Backups
- Configurations of all devices covered by this Standard will be backed up using a reliable, scheduled, automated process. Minimum requirements:
- Three months' worth of backups available for restore.
- Where possible, automated backups triggered after any configuration change.

Note: - Network Device includes Only Managed Network Switches as firewall backup and configuration part has been managed by Parent company Arrow.

1.2.2 Network Time Synchronization

- The synchronization of network device clocks is critical to ensure the accuracy of event, system, and audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.
- The Network Time Protocol (NTP) provides a mechanism to synchronize time on network devices and is required to be enabled on all devices that support it.

1.2.3 Managing Networks

- Suitably qualified staff is to manage the organization's network and preserve its integrity in collaboration with the nominated individual system owners. Information Security issues to be considered when implementing policy include the following:
- Inappropriate control over access to the network will threaten the confidentiality and integrity of your data.
- Adequate capacity shall be ensured for efficient operation.

1.2.4 Managing Wi-Fi Network

- All wireless access points must be centrally managed for configurations, updates, and policies.
- The BeyonData Solutions Pvt. Ltd. Wi-Fi infrastructure must provide the capability to detect and report on rogue wireless access points.
- All authentication methods, policies, and authorization must be centrally controlled and managed.
- Corporate Wi-Fi Access
- Have the same access as other devices directly connected in BeyonData Solutions Pvt. Ltd. intranet network.
- Utilize the same Internet protections as other devices directly connected to BeyonData Solutions Pvt. Ltd. Intranet network.
- Only allow BeyonData Solutions Pvt. Ltd. owned devices to connect and require user and machine level authentication.
- Guest WI-Fl Access
- There will be a captive portal page requiring all users to agree to the terms of use.
- Guest Wi-Fi must have the ability to associate an IP address with a wireless MAC address. traffic.
- Web filtering must be implemented on Guest Wi-Fi to protect devices on the wireless network and BeyonData Solutions Pvt. Ltd. internet connection.
- Guest Wi-Fi shall be completely isolated from the corporate BeyonData Solutions Pvt. Ltd. network

1.2.5 Site to Site Tunnel

- Site to site tunnels for business-to-business connections or cloud-based vendors are defined as encrypted tunnels.
- Traversing, the Internet to or from BeyonData Solutions Pvt. Ltd. perimeter firewalls and another business partner. Minimum security used for site-to-site IPSEC tunnels:
- Encryption will be AES with a 256bit key (or higher) using either GSM or CDC.
- Authentication will use SHA2 with a 256bit key (or higher).
- Additional Information:
- SHAl, MD5, DES, RC4 must not be used.
- Any other encryption algorithm or hash function with a key length below 256 must not be used for encryption or authentication of IPSECNPN tunnels.

1.2.6 Accessing your Network Remotely.

Remote access to the organization's network and resources will only be permitted providing that authorized users after an approval of their Reporting manager Client Based VPN Access BeyonData Solutions Pvt. Ltd. Employees and Contractors with BeyonData Solutions Pvt.

Ltd. Managed Device BeyonData Solutions Pvt. Ltd. employees and contractors' workers that have been provided BeyonData Solutions Pvt. Ltd. network credentials, BeyonData Solutions Pvt. Ltd. Managed laptops and desktops devices will have full access to the BeyonData Solutions Pvt. Ltd. corporate networks and systems via client-based VPN. Access to the corporate network for these individuals and systems must meet the following requirements for access:

Individuals

- Active network account (BeyonData Solutions Pvt. Ltd. Active Domain Account only allow)
- Use an MFA (Multi Factor Authentication)
- Use their own named account (no service accounts or share account access) Systems.
- Laptops/Desktops must:
  - Be a member of an BeyonData Solutions Pvt. Ltd. corporate domain.
  - Have a Windows or Mac OSX operating system with current patches and updates install.
  - Have the local system firewall enabled and Global Protect VPN client installed.

Consultant Workers with Non-BeyonData Solutions Pvt. Ltd. Device

Consultant workers provided with BeyonData Solutions Pvt. Ltd. network credentials but using devices not managed or maintained by BeyonData Solutions Pvt. Ltd. will be provided with network access on an exception basis. Access will be provided through user groups and firewall exceptions to eInfoctrips corporate systems and networks. These users will access a specific VPN portal and will need to meet the following requirements:

Individuals

- Active network account.
- Use an MFA (Multi Factor Authentication)
- Use the provided named account (no service accounts or share account access).
- Be a member of a group given specific access to BeyonData Solutions Pvt. Ltd.

Systems

- Laptops/Desktops must:
  - Have a Windows or Mac OSX operating system with current patches and updates.
  - installed.
  - Have the local system firewall enabled.
- Network Access:
  - Network access will be provided through group membership.
  - Network access will be by exception only to designated and approved internal BeyonData Solutions Pvt. Ltd. systems and networks.
  - Enterprise Security Risk and Architecture teams will review new requests for approval before access is granted.
  - Linux based operating (Only Ubuntu 16.0) systems are supported for use with client based.
  - VPN.