IPE GLOBAL CENTRE FOR KNOWLEDGE AND DEVELOPMENT, NEW DELHI

INFORMATION TECHNOLOGY (IT) POLICY

A. PURPOSE

The purpose of this Policy is to ensure that information technology resources of IPE Global Centre for Knowledge and Development (CKD) (hereinafter referred to as "Organisation") are used 1) for business purposes consistent with the mission of the Organisation, 2) in accordance with Organisation policies, procedures, and contractual obligations, and 3) in compliance with applicable laws and regulations. It is intended to protect both the Organisation and users from possible liability and to safeguard Organisation assets and information. It applies to all users of Organisation's information technology resources. Users may be employees, clients, contractors, teaming partners, or suppliers of the Organisation.

B. ACKNOWLEDGEMENT

Employees will acknowledge the acceptance of this policy by signing an acknowledgement form annexed with this policy.

If a non-employee requires access to the Organisation's network or equipment, it is the responsibility of the employee who engages those services to provide the individual with a copy of this policy and to request that they sign the acknowledgement located on the last page of this form. The signed acknowledgment should be given to the local IT representative before access rights to equipment or systems are granted. Failure to acknowledge this policy may result in the revocation or suspension of a user's computer credentials.

For questions regarding the **IT Policy**, contact the IT Department – ckdit@ipeckd.org.

C. POLICY

Use of Organisation computers, networks, messaging systems and internet access is a privilege that may be revoked at any time for inappropriate conduct. Users are expected to act responsibly and to respect others. Examples of inappropriate conduct include, but are not limited to, the following:

- Engaging in private or personal business activities;
- Promoting non-Organisation related causes;
- Misrepresenting oneself or the Organisation;
- Engaging in unlawful or malicious activities;
- Using abusive, profane, threatening, racist or otherwise objectionable language in any message;
- Accessing, sending, receiving, storing or printing pornographic, racist or otherwise objectionable materials;
- Causing congestion, disruption, disablement, alteration, or impairment of Organisation networks or systems;
- Infringing in any way on the copyrights or trademark rights of others;
- Unauthorised or unlicensed use of software or intellectual property;
- Knowingly propagating or disseminating malicious software of any type;
- Using recreational games or gambling; and/or
- Defeating or attempting to defeat security restrictions on Organisation systems and applications.

Use that interferes with normal job functions or the ability of users to perform daily job activities is considered excessive. This Policy informs users that the tools, applications, and information created and accessed from the Organisation's computer systems are the property of the Organisation, and users should have no expectation of privacy on Organisation-owned and Organisation-administered systems.

Antivirus and other client security agents adopted for use by the Organisation are mandatory on all Organisation provided computers. They may not be removed or disabled without permission from IT department.

Users must not encrypt Organisation communications or Organisation data unless authorised to do so.

i. **Monitoring:** The Organisation provides the network, personal computers, electronic mail and other communications devices for use on Organisation work. Organisation IT resources are subject to monitoring, logging, auditing and inspection at the Organisation's discretion. Data and correspondence stored on Organisation systems may be subject to legal and administrative inquiry. The Organisation reserves the right to inspect any information including *inter alia* emails on official accounts and take back-up of the same at any time without notice.

ii. **Passwords:** Initial passwords are assigned by the IT department. Users must change their initial passwords as soon as possible using the instructions provided by the IT personnel. Users may also be required to change their passwords on a regular basis by Organisation Policy. Passwords must not be shared, stored, or displayed in locations where they could be accessible to others. Using another person's password is strictly prohibited. The Organisation reserves the right to override any employee-selected passwords and/or codes.

iii. **Electronic Messaging:** The content of all electronic messages is governed by HR policies and Employee Code of Conduct. E-mail and other means of electronic communication should be used for appropriate business purposes. It should not be used to promote outside commercial ventures; religious, social, or political causes; or other non-job-related uses. Users must not auto-forward e-mail outside of the Organisation e-mail system and must not forward work-related correspondence to personal e-mail accounts. Instant messaging programs, such as WhatsApp, MSN, Google Talk, Telegram, etc. that are not supported by the Organisation cannot be used for official Organisation correspondence and should never contain Organisation confidential information.

iv. **Legal Proceedings:** Information sent by users via the electronic mail and messaging systems may be archived and used in legal proceedings. E-mail messages are considered written communications and are potentially subject of subpoena in litigation. The Organisation may inspect the contents of e-mail messages in the course of an investigation, will respond to the legal process, and will fulfill any legal obligations to third parties.

v. **Network Security:** IT will monitor network security on a regular basis. Users are prohibited from any attempt to alter or breach the Organisation's security systems. To safeguard network security and performance, no device or network service such as computers, printers, scanners, routers, hubs, web-cams, wireless access points, or other IT-related technologies may be placed on the network without approval from IT.

vi. **Data Security:** Users are responsible for the protection of data stored on their systems; further, employees will not deface or physically alter the data stored on Organisation provided systems. It is the responsibility of each individual with an access to sensitive data (public drives) to obtain the same fairly and in responsible manner. The Organisation information should not be disclosed by any means, accidentally or otherwise to any unauthorised third party. Any accidental disclosure or suspected misuse of sensitive data should be reported immediately to the IT department/line manager. Also refer clause **vii – Periodic Backup**, below.

vii. **Periodic Backup:** The Organisation recognises that IT backup and maintenance of data for servers are critical to the viability and operations of the respective departments.

We have a central server based out of our New Delhi office where back-up of data of all users is maintained on weekly basis using Veritas Net Backup. Back-up of ERP Server and Data Server, is taken on a continuous basis using Veritas Net Backup. This back-up is taken on Tape Drives on daily basis and stored off-site on a weekly basis and monthly basis.

User Level Data Access & Storage: For the common data storage and access related activities, the users are mapped on SAN (Storage Area Network) with the drive names connected on their respective laptops which may be referred for any data storage or access activities.

viii. **Remote Access:** The Organisation has in place SonicWALL (network firewall) to allow secure remote access to organisation network by establishing an encrypted tunnel across the Internet. Remote access to the Organisation network must be accomplished over an encrypted VPN connection using a Organisation-provided VPN client or secure connection facilities as provided IT Department. Unencrypted connections

using terminal server, remote desktop, and other similar technologies are not permitted unless they traverse an already-established VPN connection.

ix. **Physical Security**: Access to server room will be limited to IT personnel only who require access for the normal performance of their jobs.

x. **Care of Equipment**: Safety and upkeep of Organisation-owned equipment including laptops implying careful handling, protection from damage and theft, etc. during the normal job functions and when the equipment is taken out of office for non-job functions, shall be responsibility of employee concerned. Users must return all equipment to the Organisation upon completion of the assignment for which it is intended, at termination, or at the request of management or IT personnel. A record of equipment issued for this purpose will be maintained by the IT Department with a copy retained in employee's personnel file.

If the Organisation-owned equipment is stolen due to negligence of employee concerned when out of office, the Organisation has right to deduct the amount from concerned employee's salary based on book value of the same as per law.

xi. **Organisation-Owned Equipment: The** Organisation equipment is meant to be used by authorised personnel for Organisation use. Equipment must not be altered in any way that would compromise the integrity of the systems, data, or security protection. Where Organisation equipment is used on client-owned premises or connected to client-owned systems and networks, it is also subject to client policies relating to equipment use. In the event that there is a conflict between the Organisation's IT Policy and that of a client's, the more restrictive policy will prevail.

xii. **Non-** Organisation **Owned Equipment**: Non-organisation owned equipment includes personal computers, laptops, personal digital assistants, digital cameras, modems, wireless access points, USB hard drives, flash cards, storage devices, etc.

Employees are discouraged from using personally owned equipment for Organisation work. The Organisation is not responsible for security, maintenance, or protection of personal equipment.

Visitors may connect computers to Organisation guest wireless network for firewalled internet access only. Equipment owned by the client, teaming partner, or supplier can be connected to the Organisation systems or networks with the explicit authorisation of IT department.

The Organisation reserves a right to inspect non-organisation owned equipment attached to Organisation networks or systems. Inspection includes the monitoring of its use and analysing any files, data, or systems which it may contain. The Organisation information stored on this equipment remains a property of Organisation. It is subject to the Organisation's policies on confidentiality and must be removed on Organisation's request. Non-organisation owned equipment may be disconnected from Organisation-owned resources or networks by the IT staff without the permission of or notice to the user.

xiii. **Internet Use**: Internet access is provided to users for organisation work. Any personal use should be incidental and should not interfere with the performance of an individual's job function. Users with internet access are expressly prohibited from accessing, viewing, downloading, uploading or printing violent, pornographic, sexually explicit, or other materials that may be considered offensive, as outlined elsewhere in this policy. In addition, users should be mindful that there is no assurance that e-mail text, attachments, or other Organisation information sent or posted within the Organisation and on the internet will not be seen, accessed, or intercepted by unauthorised parties.

xiv. **Information Sharing**: Sharing the Organisation information on the internet or other publicly accessible forums is subject to the Organisation's policy on confidentiality and is only allowed within the context of the user's duties.

xv. **Software Usage**: Users are expected to use Organisation-authorised and provided software. All software is to be used in accordance with the terms of the applicable software licenses. In order to protect the integrity and security of the Organisation's systems, users are not permitted to install applications, demos, or upgrades without the prior approval of their manager or their IT department. Software purchased by the

Organisation shall not be installed on employee-owned or other third-party computers unless those installations are authorised by Organisation management, and then only after the appropriate licenses are procured. Conversely, employee-owned software must not be installed on Organisation-owned computers.

D. CONSEQUENCES OF VIOLATION

Failure to comply with this policy governing the use of IT equipment may result in consequences which could include the revocation of user access and privileges, seizing or removal of equipment, employee discipline up to and including termination, and possible civil or criminal penalties.

E. POLICY REVISIONS

Any revisions in this Policy including amendments or changes under respective clauses will be duly notified to employees through email communication. Also, such revised Policy or notification/ circular/ internal communication on such revisions will be updated in Darwinbox (HR ERP) and the Organisation Website (www.ipeckd.org). The employee shall be deemed to have read, understood and acknowledged the changes thereof which will supersede the terms of current Policy or any subsequent document/communication related to the Policy.

IT POLICY ACKNOWLEDGMENT

After reading this policy, please sign this acknowledgement form and submit the same to IT department for filing.

By signing below, the individual requesting Organisation computer and/or network access hereby acknowledges receipt of and compliance with the IT Policy. Where this policy references outside policies (i.e. HR Manual), it is the responsibility of the user to request copies of the appropriate policy. Furthermore, the undersigned also acknowledges that he/she has read and understands this policy before signing this form.

Computer and/or system access will not be granted until this acknowledgment form is signed by the individual. After completion, the form is filed in the individual's human resources file (for full time employees), or in a file specifically dedicated to IT Policy Forms (for contract workers, etc.), and maintained by the IT Department.

This acknowledgment form is subject to internal audit.

Location: _____

Department: _____

Name: _____

Employee (Consultant, Contractor or Other): _____

If Employee, Employee Code: _____

Signature: _____ **Date:** ____/____/____