# 1.0 Introduction

Keeping the information assets of the organization secure is vital to the success of the business. All leading organizations have the driving imperative to improve the degree to which they protect the conﬁdentiality, integrity and availability of information systems and critical business data. Additional complexity comes from the need to maintain legal and/or regulatory compliance, corporate governance and remain ﬂexible to survive in today’s hyper competitive marketplace.

Threats to organization’s information assets may be external or internal. And to control the inside or outside threats, organization may need to put technological and/or management system controls; whereas special focus should be given on employees who are un-informed about information security. Being not informed, these employees may un-intentionally harm the organization and/or IT systems by visiting websites infected with viruses, responding to fraud emails, storing their password in an unsecured location leading to data theft, giving out sensitive information over the phone when exposed to social engineering or even downloading copyright material without being aware of its legal implications and penalties.

# 2.0 Purpose

The purpose of this policy is to establish the appropriate use i.e. acceptable use of information assets at iBoss Tech Solutions Private Limited(referred to as “iBoss” in rest of this document) in conjunction with its established culture of ethical and lawful behavior, openness, trust and integrity. The information assets and related resources are owned/leased/rented by the iBoss and are provided primarily to enable/facilitate the oﬃcial duties and responsibilities of the intended users. This policy sets out the responsibilities and limitations on the use of the iBoss’s information assets and the intention is to avoid any unauthorized use which may cause damage to the system, loss of data or criminal and/or civil liability for you and/or for the iBoss.

# 3.0 Scope

This policy applies to employees including trainees, contractors, consultants and all personnel using IT resources of iBoss under their governance. This policy applies to all information assets that are owned or leased by iBoss. The information assets are (including but not limited to) data, design or engineering details, business proposals, operational and ﬁnancial data, the business processes, hardware or software resources, computing and telecommunication networks, IT resources and/or customer supplied assets but anything and everything that has value to iBoss.

# 4.0 Enforcement

Effective security is a team effort involving the participation and support from every level. Thus all employees and/or information asset user(s) need to adhere to this policy. Any employee including trainees, contractors, consultants and all personnel using IT resources of IBoss under their governance, found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract or agreement as the case may be. Violation of this policy may also invite legal implication in accordance with applicable law.

# Policy

* 1. **General Use and Ownership**
     1. All users are responsible for exercising good judgment regarding appropriate use of all information assets in accordance with iBoss’s policies, procedures, standards, and guidelines.
     2. IBoss’s information assets and IT resources must not be used for any illegal or prohibited purpose.
     3. All users are responsible for ensuring the protection of assigned information and information processing facilities.
     4. Use of facilities, services and information assets for personal commercial purposes is prohibited.
     5. Do not create, circulate, forward, distribute, store and/or download any material or make any statements:-
        + which may be considered to infringe the iBoss's Equal Opportunities approach or be in any way discriminating or harassing (whether sexually, racially or otherwise).

which may result in ﬁnancial or legal liability or may in any manner damage the reputation of the iBoss.

# Data / Information

* + 1. Do not save business critical data on local hard drives; rather always save it on centralized server.
    2. Folder sharing must be restricted to business need-to-know basis and always consider periodic review to revoke any unauthorized access.
    3. Do not send any oﬃcial data/information to internal/external users for the non-business related purpose. All efforts must be made to ensure conﬁdentiality of the data being handled.
    4. Do not try to access or copy data from systems to which you are not allowed.
    5. While doing any bulk printing such as printing of manuals, e-books etc; Judicious discretion should be exercised to minimize such requirements. Saving on paper helps save our environment.
    6. Don’t fraudulently make, sign, seal, or execute a false document or false electronic record.
    7. Providing information about, or lists of, iBoss’s employees to parties outside iBoss is not allowed.
    8. The employees or any information asset user shall not use, quote, reproduce, duplicate, display, distribute, refer any patent / copyrighted work owned by iBoss or use any derivative information relating to the iBoss.
    9. The employees shall not develop patents / copyright works that are detrimental to the interest of the iBoss.
    10. The employees, trainees or third party contractors shall surrender all original written materials, including any reports,

studies, designs, drawings, speciﬁcation, documents, software, computer based training modules, electronically or magnetically recorded material used to develop software and / or software code and related intellectual property to iBoss on termination/expiry of his/her services, agreement or contract.

# Software

* + 1. Do not install / uninstall any software and/or unauthorized mobile code(s) on/from the iBoss’s computer without the prior

approval from IT department. This includes software’s like MS Oﬃce, Screensavers, Games (except for default games loaded with windows operating system), time managers, messengers and other software utilities, etc.

* + 1. Use of pirated software is strictly prohibited on any computer system of iBoss and also the media containing such software must not be brought in the iBoss’s premises.
    2. Do not circulate, forward, distribute, store or duplicate an executable ﬁle of any software on your computer systems unless explicitly required for business purposes.
    3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal and thus strictly prohibited. The iBoss Head should be consulted prior to export of any material that is in question.

# Desktop and/or Laptop

* + 1. Do not leave your computers logged in and unattended for long durations. Whenever you are leaving your computer unattended then either it must be logged off or it must be locked (Ctrl+Alt+Del).
    2. Individual computer must be switched off before leaving the oﬃce everyday (unless required for oﬃcial reasons).
    3. Do not make any changes to the hardware conﬁguration of IT devices and any changes noticed must be reported immediately to IT department.
    4. Ensure to update latest antivirus deﬁnition and approved windows patches on your computer / laptop.
    5. Before putting your laptop in its bag, ensure that it is turned off, all lights are out, all external cables are unplugged and no removable media is plugged in.(In any case, it should not be in hibernate or in stand-by option).
    6. Do not allow a laptop issued for business purposes to be used by family or friends.
    7. While doing an air travel, laptop should be carried in cabin luggage and should not be put in check- in luggage.
    8. If the laptop is lost or stolen, it should be reported immediately toiBoss.
    9. Do not place heavy objects on the laptop and handle the laptop with care.

# Media Management

* + 1. All the media such as hard-disks, USB, CD/DVD, etc containing business relation data/information must be protected and stored in safe and secure environment to ensure conﬁdentiality, integrity and availability.
    2. Backup of information (if necessary) must be ensured before disposing of the media.
    3. Disposing of information must take place in an appropriate manner which may include shredding of paper documents & crushing of optical media.
    4. Bringing and using personally owned computing devices such as laptop, pen drives, data cards, CD/DVD, hard-disks, etc

inside iBoss premises is strictly prohibited unless explicitly approved in written by unit head.

# Email

* + 1. When communicating on oﬃcial email system, utmost care has to be taken as well as high professional standards must be followed because you are representing iBoss while sending or replying on oﬃcial mail id.
    2. Users are fully responsible for the professional, ethical and lawful use of email and other information systems.
    3. No personal email id must be used to interact for oﬃcial reasons with (including but not limited to) vendors, customers, service providers or partners. Only oﬃcial email id must be used to do any oﬃcial email correspondence.
    4. Employee should not use oﬃcial mail id for personal use. Further it is employee’s responsibility to discourage receiving personal mails on oﬃcial email id. (However occasional personal mails may be allowed, in emergent situations only).
    5. Employees must use extreme caution when opening e-mails and speciﬁcally attachments received from unknown senders, as these may contain viruses, worms or Trojan horse code. In case of any suspicion, immediately inform IT department.
    6. Forging of email headers is prohibited. Similarly sending emails from someone else computer without the prior written approval of that user is not allowed.
    7. Postings by employees of iBoss to any newsgroup/blogs/online-communities using oﬃcial email address (or through any

other content which reﬂects the concerned persons relationship with iBoss) shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of iBoss). The only exception to this rule would happen incase such postings is in the course of business duties and have been explicitly approved by iBoss.

* + 1. IBoss’s policy strictly prohibits creating, circulating, distributing, storing and/or downloading (internally or externally) any:
       - Chain letters;
       - Religious, political or business solicitations which do not relate to your duties as an employee;
       - Any ﬁles (including games, screen savers, .jpg or .wav or .mp3 or .scr or .bin or .zip ﬁles or other software and shareware) which are not business related.
    2. User must save at least all their business important mails, such as approval mails, important discussion mails, etc as records at centralized server location covered under backup.

# User Access & Password Management

* + 1. Each user is provided with a unique individual user id; while password can be selected by user themselves. Passwords must not be shared with anyone.
    2. User is solely responsible for all actions conducted by using his/her user id. Thus it is expected to take all necessary steps

to protect misuse of user id, which is not limited to periodically changing of password, ensuring password is complex and not easily guessable etc.

* + 1. Users will not make any attempt to gain unauthorized access to restricted ﬁles or networks, or to damage or modify computer equipment or software.
    2. Users are precluded from installing, removing or editing scripts which affects system conﬁguration and functionality.
    3. Any unauthorized action that causes a system to malfunction or disrupts the normal performance of the system and /or the connected terminals is a security violation, irrespective of the system location or time duration.
    4. Users will respect the privacy of other users, and will refrain from unauthorized attempts to view or read material being used by others.

# Internet

* + 1. User is responsible for the usage of internet made by his/her internet/windows account and thus user must take reasonable steps to ensure that others do not gain unauthorized access to his/her internet/windows account.
    2. Internet must not be used for illegal activity, to access illegal materials, or to access/publish materials that are obscene/pornographic/sexually explicit material.
    3. Downloading copyright protected material including software or freewarefrom the internet, without appropriate written authorization by Head of Department, is prohibited.
    4. No online storage accounts such as yahoo briefcase, etc must be accessed to store information.
    5. User must not indulge into downloading unreasonably large ﬁles such as streaming audio & video ﬁles which may lead to disruption in network services.
    6. User must refrain from engaging in any activity that in anyway bring disrepute, or can lead to litigation upon iBoss.
    7. User must not indulge in publishing defamatory and/or knowingly false material about iBoss, colleagues and/or our customers on internet including social networking sites, ‘blogs’ (online journals), ‘wikis’ and any online publishing format.
    8. To ensure security and avoid the spread of viruses, user must not bypass iBoss’s network security by accessing the internet

directly by modem, CDMA, GPRS, 3G or other means. This is strictly prohibited unless the computer you are using is not connected to the iBoss’s network.

# Remote Access

* + 1. It is responsibility of employees with Remote Access privileges (setup and managed by IT department) to ensure that access is not shared with any unauthorized users for iBoss’s internal networks and information assets.
    2. It is the responsibility of employee to ensure that the computer, used to connect to iBoss’s network via: VPN or any other technology or medium, is updated with antivirus software and its latest deﬁnition.

# Network / e-Security

* + 1. All users are responsible for the security and appropriate use of company’s network resources under their control.

UsingiBoss resources for the following is strictly prohibited:

Causing a security breach to network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniﬃng network traﬃc.

Transmitting on or through any of the iBoss’s services, any material and/or message that is illegal, false, obscene,

threatening, sexual or obscene nature, defamatory, offensive, abusive, hateful, or encourages conduct that could constitute a criminal offense, give rise to civil liability, or otherwise violate any local, national or international law.

Causing a disruption of service to network resources, including, but not limited to, ICMP ﬂoods, packet spooﬁng, denial of service, heap or buffer overﬂows, and forged routing information for malicious purposes.

Indulging in any illegal activity and/or crime such as breach of conﬁdentiality and leakage of data, introducing malicious programs, video voyeurism, e-commerce frauds like impersonation commonly known as phishing, identity theft, etc.

Executing any form of network monitoring, port scanning, network or security scanning is strictly prohibited.

* + 1. Allowing unauthorized or a third party to access iBoss’s network and resources, without appropriate authorization from department head, is strictly prohibited.

# Monitoring & Privacy

IBoss has full respect for individual privacy and rights. However, users should not have any expectation of privacy in respect of your usage of iBoss’s information asset and IT resources. The iBoss’s IT resources are the backbone for running the iBoss’s business and it is vital that nothing is done to compromise this in any way even if this is unintentional. Please note that the iBoss may monitor or keep a record of communications (at any time with or without notice) either directly or via an external agency and/or record your use of the IT Resources in order to (including, but not limited to):

* + - To detect/investigate any unwanted elements like virus etc which might be destructive in nature,
    - Detect and/or prevent crime,
    - Ascertain and/or demonstrate whether you and/or the iBoss are complying with the iBoss’s rules and policies (including, but not limited to, this policy) and also with legal and/or regulatory obligations which you and/or the IBoss are subject to;
    - Ascertain whether communications are relevant to the iBoss’s Business,
    - Ascertain and/or demonstrate whether the iBoss is attaining appropriate standards of customer service.

The iBoss will, in conducting such monitoring activities, use all reasonable endeavors to comply with regulatory guidelines and to respect your privacy using the IT Resources.

# Declaration & Acceptance

I ANAND PRAKASH

Resident of VILL AND POST DAMKHODA TEHSHEEL-BHAERI DISTRICT BAREILLY PIN-243201 ,

Hereby agree, acknowledge and conﬁrm that:

* IBoss reserves the right to revise, amend, or modify this policy at any time and in any manner. However, notice of any revision, amendment, or modiﬁcation will be notiﬁed to all personnel via: email.
* Reading and practicing of any future release(s) of this policy, on periodic basis, is solely my responsibility; however understanding of any part of this policy shall be provided on my written request to the HR department.
* The provision(s) and obligation(s) of this policy, and its future release(s), shall apply and continue in effect for a period of my employment/contract from the date hereof.
* The provisions hereof shall be governed and construed by the iBoss, and by my acceptance hereof I agree that I have understood this policy to my satisfaction.

Name ANAND PRAKASH

Emp. ID CND42

Date 15/07/2022

Signature ANAND

*Please indicate your acceptance of the above by signing and returning the enclosed copy of this policy to HR Department.*