IPC Acceptable Use Policy

Rev 1.6 December 5, 2025

Author:	**John Gardner Chief Information Security Officer**
Department:	**Information Security**
Effective Date**:**	**July 6, 2022**
Data Classification:	**IPC Proprietary**

Purpose

InfoSec is committed to protecting IPC's Employees, Partners, Customers, and the Company from illegal or damaging Information Security actions by individuals, either knowingly or unknowingly. To ensure the protection of IPC's information and Information Assets, the Information Security Office has established information security requirements that pertain to acceptable and unacceptable use of IPC's assets associated with information and information processing facilities and resources. IPC's Acceptable Use Policy encompasses all Information Assets.

The *IPC Acceptable Use Policy* must be signed by every employee as part of the onboarding process upon hire.

Acceptable Use – Do's

The following are acceptable uses of IPC Information Technology Assets and Resources.

- **IPC Assets**: IPC Information (that of IPC, its Customers and Partners) stored on electronic and computing devices whether owned or leased by IPC, the employee or a third party, remains the sole property of IPC.
- **Loss or Theft**: Employees and Contractors must Promptly report the theft, loss or unauthorized disclosure of IPC Information.
- **Personal Use**: Employees and Contractors are responsible for exercising good judgment in what is regarded as reasonable personal use. Personal use which puts an Information Asset at risk is prohibited. If there is any uncertainty around personal use, employees should consult their supervisors.
- **Compliance to Controls/Policies**: All devices connecting to the IPC Corporate Network or Any other IPC Managed, or Controlled Network must comply with all Security Controls and Policies.
- **Lock Screen**: All computing devices must be physically secured and logically secured with a password-protected screensaver. You must lock the screen or log off when the device is unattended.
- **Confidential Documents**: It is your responsibility to protect IPC Information within your control (including but not limited to customer data, proprietary data, product information, financials, etc.). Put away confidential documents!
- **Document Classification/Label**: Information in PDF, Word, Excel, and other formats (electronic, digital, or paper) should be appropriately labeled with an Information Classification Level.
- **Adherence to Information Security Training/Anti-phishing Guidelines**:

  - Don't click on any link or open any file attachments from an unknown sender or email address.
  - Never provide your credentials in an unexpected email.
- **Additional Guidance**: In addition to the above, IPC has specific policies for:
  - Personal Electronic Device Policy
  - Cloud File Sharing and Synchronization Policy
  - Removable Media Policy
  - Customer Data Management Policy
- **Use of AI Tools:** Confidential information shall only be uploaded to approved AI tools. If you think an AI tool has shared or exposed information by mistake, you must report it to Information Security immediately.

Unacceptable Use – Do Not's

The following activities are, in general, prohibited unless your job role includes these responsibilities or requires you to perform these actions. Under no circumstances is an employee of IPC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing IPC-owned resources. The prohibited activities listed below are by no means exhaustive but attempt to provide a general understanding and framework for activities which fall into the category of unacceptable use.

1. **Unauthorized Installation of Devices**: Installing any device on the IPC Corporate IT Network which is not authorized by Corporate IT and Information Security.
2. **Unauthorized Installation of Software**: Unauthorized installation of any software, especially copyrighted software for which IPC or the end user does not have an active license.
   - Messaging applications for example WhatsApp, Slack, Telegram and Signal are not to be installed on IPC Computers unless specific exception is documented.
   - Unapproved Software will be removed wherever found.
3. **Unauthorized Account Access**: Accessing data, a server, or an account for any purpose other than conducting IPC business, even if you have authorized access.
4. **Unauthorized Access to Email or Teams Chats**: Access to Email or Teams Chats (Including Reading or Copying) other than your own shall require a ticket from HR, Legal or Risk with the approval of IT Leadership.
5. **Unauthorized Storage/Transfer of Data**: Storing or Transferring IPC Data or IPC Customer Data outside of authorized IPC Storage or Transmission Mediums.
6. **Unauthorized Changes to IPC Assets:** Tampering with IPC Computer Assets or Destroying or Manipulating IPC Data in any way without Information Security, Corporate IT or Management Approval

   This includes but is not limited to:
   - Making physical changes to Computer Assets

- Making changes to Operating Systems or Underlying Hard Drive Formatting
- Removing or Destroying IPC Data Assets (Including Data on Computers Assigned to Individual Employees)
- Obfuscating or Hiding IPC or IPC Customer Data Assets

7. **Violation of International/Regional Export Laws**: Unauthorized Export of Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to the export of any material that is in question.
8. **Distributing Malware**: Introducing malicious programs into IPC's network (e.g., viruses, worms, Trojan horses, email bombs, etc.).
9. **Disclosing of Passwords**: Under no circumstances are Accounts or Passwords to be shared. Account and Password sharing is expressly prohibited in all cases.
10. **Fraudulent Use of IPC Email**: Unauthorized use or fraudulent use of IPC Email.
11. **Unauthorized System or Network Access**: 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. Note: 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.
    - **Network Probing**: Performing Port or Security Scans without explicit approval from the InfoSec Office.
    - **Network Monitoring**: Executing any form of network monitoring, unless this activity is a part of the employee's normal job/duties.
    - **User Authentication**: Circumventing user authentication or security of any host, network or account.
    - **Decoy Servers**: Introducing Honeypots (decoy servers or systems setup to gather information regarding an attacker or intruder into your system), Honeynets (a network set up with intentional vulnerabilities), or similar technology on the IPC network.
    - **Denial of Service**: Interfering with or denying service to any system/user (Denial of Service attack).
    - **User Sessions**: Using any programs, scripts, commands of any kind with the intent to interfere with, highjack, piggyback, ghost, or disable a user's session.
    - **Distribution of IPC Information**: Copying or distributing any IPC Information/data in any form to unauthorized individuals/parties. It is prohibited to release any IPC data/information to anyone who is not authorized or to anyone who the information is not meant for.

References

Personal Electronic Device Policy

Cloud File Sharing and Synchronization Policy
Removable Media Policy
Customer Data Management Policy

Revision History

Ver.	Purpose of Change	Changed By:	Date
1.0	Initial release	John Gardner, Chief Information Security Officer	24-Jun-22
1.1	Added - Unauthorized Changes to IPC Assets	John Gardner, Chief Information Security Officer	27-Mar-23
1.2	Added emphasis on the prohibition for the sharing accounts or passwords	John Gardner, Chief Information Security Officer	19-Sep-23
1.3	Added messaging application install restriction & removal of unapproved software	John Gardner, Chief Information Security Officer	15-May-24
1.4	Added restriction to access to Email and Teams Chats	John Gardner, Chief Information Security Officer	8-JUL-24
1.5	Font update requested by HR	John Gardner, Chief Information Security Officer	2-DEC-24
1.6	Added use of AI tools	Cristina Ceballos Herrero, Compliance & Governance Manager	5-DEC-25