




ACCEPTABLE USE POLICY

Enterprise Risk Management and Compliance Department

Document Edit History

Version	Author	Section Affected	Remarks	Reviewed by	Approved by	Date Approved
1.0	Information Technology Department - <i>Aventus</i>	ALL	Initial Policy	Mr. William Montalbo, IT Senior Manager	Mr. Wenefrido Fernando, AVP of Operations	23-Jun-2016
1.0	Information Technology Department - <i>Asalus</i>	ALL	Initial Policy	Mr. Melanio Felix Garcia, Assistant Vice President-IT Head	Mr. Arnaldo Dantis, VP of Operations	01-Feb-2019
2.0	Information Technology Department - <i>Asalus</i>	ALL	Restructure/ Reformat Document	Mr. Melanio Felix Garcia, Assistant Vice President-IT Head	Mr. Arnaldo Dantis, VP of Operations	20-Jan-2020
2.0	Information Technology Department - <i>Aventus</i>	ALL	Revision into the new policy template	Mr. William Montalbo, IT Senior Manager Dr. Cheryl Ann Rueca, Medical Risk Officer	Mr. Wenefrido Fernando, AVP of Operations Mr. Jeremy G. Matti, President - Asalus Corporation & Aventus Medical Care Inc.; Mr. Mark B. Gamir, President - Avega Managed Care Inc.	17-Mar-2021
3.0	Enterprise Risk Management and Compliance Department	ALL	- Change of Ownership - Additional Provisions	Ms. Desiree Nica F. Alibio, AVP-Operations and Health Care Risk Officer	Mr. Jeremy G. Matti, President - Asalus Corporation & Aventus Medical Care Inc.; Mr. Mark B. Gamir, President - Avega Managed Care Inc.	05-Aug-2021
3.1	ERMCD	ALL	- As a result of review, no significant changes were made in the policy.	Ms. Desiree Nica F. Alibio, AVP – Operations and Health Care Risk Officer	IT Steering Committee; Risk Board Committee	11/03/2022

Version	Author	Section Affected	Remarks	Reviewed by	Approved by	Date Approved
3.2	ERMCD	ALL	As a result of review, no significant changes were made in the policy.	Ms. Desiree Nica F. Alibio, AVP – Risk & Information Security Officer	MR. JEREMY MATTI Chairman, IT Steering Committee Risk & Compliance Board Committee*	July 19, 2023
3.3	Enterprise Risk Management and Compliance Department	ALL	No significant changes were made in the policy as a result of annual review	Ms. Desiree Alibio, AVP-Risk and Information Security Officer	MR. JEREMY MATTI Chairman, IT Steering Committee Risk & Compliance Board Committee*	February 13, 2024
4.0	Enterprise Risk Management and Compliance Department	ALL	Merged Information Security Workstation Policy.	 Desiree Alibio, Assistant Vice President – Risk and Information Security Officer	 MR. JEREMY MATTI Co-Chairman, IT Steering Committee  MR. NORMAN AMORA Co-Chairman, IT Steering Committee Risk & Compliance Board Committee*	January 28, 2025 February 20, 2025

*Approval of the policies attested and certified by the Director and Chairman of the Risk & Compliance Board Committee. Separate document for the certification.

1. INTRODUCTION

1.1. Policy Statement

Information Security under Enterprise Risk Management and Compliance Department (ERMCD) aims to publish an Acceptable Use Policy (AUP) to ensure adherence to Intellicare Group's established culture of trust and integrity. ERMCD is committed on protecting employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP are property of Intellicare Group. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Intellicare Group's employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable usage of computer equipment at Intellicare Group. These rules are in place to protect the employee and Intellicare Group. Inappropriate use exposes Intellicare Group to risks including malwares, virus attacks, compromise of network systems and services, legal issues. Thus, the policy must foster an environment that allows employees the independence to do their jobs while at the same time reducing the risk of data breaches, cyberattacks, and compliance violation.

1.2. Policy Owner

Enterprise Risk Management and Compliance Department of Intellicare Group.

1.3. Policy Review

The Enterprise Risk Management and Compliance Department (ERMCD) is the designated owner of the Acceptable Use Policy and therefore responsible for its review. This policy is subject for periodic review annually.

1.4. Approval Authority

Any changes to this policy have to be approved by the Risk and Audit Board Committee

1.5. Records Management

Records being created, collected, and extracted as part of this Policy shall be retained for a period of five (5) years. Records shall be in hard copy or electronic media. The records shall be owned and safe kept by ERMCD.

2. SCOPE

This policy applies to all employees, contractors, consultants, temporary and other workforce of Intellicare Group, including all personnel affiliated with third-parties. Moreover, this policy applies to use of all information systems, company's equipment, workstations, electronic and computing devices, peripherals, information media, licensing and copyright and communication infrastructure.

This policy is not limited to hardware, software, database and server access, network communications including the internet but also applies to all external communications via e-mail or other electronic media which relate to company business or involve company resources – whether communications forum or medium is the public internet, social website, instant messaging or any similar medium.

3. DEFINITION OF TERMS

The following terminologies will be a helpful tool for the users of this Policy:

- **Auto forwarding** – Capability to automatically forward e-mail onto another e-mail account immediately upon receipt.
- **Blogging** – A process of writing a blog, an online journal in which you share your thoughts about a particular subject with readers.
- **Computing Devices** – Electronic devices which take inputs, process the inputs and then calculate results from the inputs.
- **Extranet** – An intranet that can be partially accessed by authorized outside users, enabling business to exchange information over the Internet securely.
- **File Transfer Protocol (FTP)** – a protocol designed for transferring files over the internet.
- **Honeynet** – a network setup with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.
- **Honeypot** – a network-attached system setup as a decoy to lure cyber attackers and to detect, deflect or study hacking attempts in order to gain unauthorized access to information systems.
- **Instant Messaging** – A form of communication that offers and instantaneous transmission of text.
- **Intranet** – A local or restricted communications network, especially a private network created using World Wide Web software.
- **Malware** – Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Network Resources** – Refer to forms of data, information and hardware devices that can be accessed by a group of computers through the use of a shared connection. Also known as shared resources.
- **Spam** – also known as 'junk e-mail'. An unsolicited message sent in bulk by e-mail. Most e-mail spam messages are commercial in nature. Whether commercial or not, many contain disguised links that appear to be for familiar websites but in fact lead to phishing websites or sites that are hosting malware.
- **Virus** – A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

4. ROLES AND RESPONSIBILITIES

An Acceptable Use Policy (AUP) is an integral part of organization Information Security Policy. It is one of few documentations that can physically show “due diligence” with regards to the security of the network and for the protection of sensitive information and client data in the event of a breach or regular audit. Thus, policy provides statements as to what behavior is acceptable from users or employees that work in or are connected to the network.

The information contained within is for use solely by authorized Intellicare Group employees with a need to know it, should not be disclosed to others.

4.1. Enterprise Risk Management and Compliance Department (ERMCD)

- 4.1.1. Appointed as the Information Security Office (ISO) of Intellicare Group.
- 4.1.2. Shall be responsible for the management, maintenance, implementation and accuracy of the policy. Any questions regarding the policy should be directed to ISO of ERMCD.
- 4.1.3. Shall be responsible for the review, checking, reporting and monitoring of compliance.
- 4.1.4. Shall be responsible for the review and endorsement of exceptions.
- 4.1.5. Shall be responsible for the review, monitoring and safe keep of all signed Acceptable Use Policy Form for employees and Third-Parties.
- 4.1.6. Shall endorse identified noncompliance or violation to HCMD.

4.2. Human Capital Management Department (HMCD)

- 4.2.1. Shall be responsible for the dissemination of Acceptable Use Policy (AUP) as part of the on-boarding process.
- 4.2.2. Shall be responsible for gathering the employees’ signed AUP Form which forms part of the Employee Onboarding Checklist. In addition, the signed Employee AUP Forms must be submitted to ERMCD on a monthly basis - every first Friday of the following month.
- 4.2.3. Shall work hand-on-hand with ERMCD as to the compliance monitoring of all employees.
- 4.2.4. Shall assist in the sanction implementation in accordance with the Intellicare Group’s Code of Discipline.
- 4.2.5. Shall be responsible for filing of employee’s notice of noncompliance in 201 file.

4.3. Facilities and Property Administration Department or Admin Department

- 4.3.1. Shall be responsible for reiteration of Acceptable Use Policy to the third-parties/visitors.
- 4.3.2. Shall be responsible for securing a signed AUP Forms from Third-Party which forms part of the vendor onboarding process. In addition, the signed third-party AUP Forms must be submitted to ERMCD on a monthly basis – every first Friday of the following month.
- 4.3.3. Shall work hand-on-hand with ERMCD as to the compliance monitoring of all third-parties/visitors.

4.4. Department Head

- 4.4.1. Shall be responsible for ensuring that all employees under his/her department are aware of the Acceptable Use Policy.

- 4.4.2. Shall be responsible for ensuring that all employees under his/her department has a signed AUP Form for employees and direct reports are complying with the provisions statement in AUP.
- 4.4.3. Shall be responsible on serving the sanctions for information security violation/non-compliance, with the Intellicare Group's Code of Discipline.
- 4.4.4. Shall be responsible for securing AUP Forms for the Visitors of their Department who will utilize the information assets or systems of the company. The signed AUP Forms of the Visitors shall be submitted to ERMCD the following day of the visit.
- 4.4.5. Shall be responsible for justifying and monitoring the request for exceptions.
- 4.4.6. Shall report and monitor incidents within their department relating to the Intellicare Group's Acceptable Use Policy. Incident reporting process and measures must adhere to Intellicare Group's Incident Reporting Policy.
- 4.4.7. Shall work hand-on-hand with ERMCD as to the compliance monitoring of all employees within their jurisdiction.

4.5. Users

- 4.5.1. Shall be responsible for maintaining the confidentiality, integrity, availability, reliability, and efficiency of computer-based information resources.
- 4.5.2. Shall refrain from seeking to gain unauthorized access or exceed authorized access.
- 4.5.3. Shall respect software copyright and licenses and other intellectual property rights.
- 4.5.4. Shall be responsible and liable for all the activity made using his/her company assets (e.g. company laptop, company desktop, company mobile device, etc.) and account credentials.
- 4.5.5. Shall ensure that they have signed the AUP Form for Employees and ensure compliance to the provisions stated.
- 4.5.6. Shall ensure understanding and compliance to the periodic releases of Intellicare Group eLearning Awareness Programs.
- 4.5.7. Shall report suspected violations of AUP to ERMCD of Intellicare Group.

4.6. Third-Parties or Visitors

- 4.6.1. Shall be aware and adhere to the Acceptable Use Policy of Intellicare Group.
- 4.6.2. Shall only use those computing and information technology resources for which they have authorization and only for their intended purpose.
- 4.6.3. Shall abide by the policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

4.7. Information Technology Department

- 4.7.1. Shall have the responsibility of ensuring the confidentiality, integrity, and availability of the resources they are managing.
- 4.7.2. Shall be responsible on creating and updating of inventory of workstations (computer/laptop), application software, and systems.

4.7.3. Shall be responsible in assisting any IT related concerns.

4.8. Internal Audit

4.8.1. Shall be responsible for scheduling and conducting of audit activity to ensure that this policy is being implemented.

5. BUSINESS RULES AND POLICIES

5.1. General Use and Ownership

- 5.1.1. Intellicare Group's proprietary information stored on electronic and computing devices whether owned or leased by the company, the employee or a third party, remains the sole property of Intellicare Group. Users must ensure through legal or technical means that proprietary information is protected in accordance with the Data Privacy Act of 2012.
- 5.1.2. Employees have the responsibility to promptly report the theft, loss, or any unauthorized disclosure of the company's proprietary information. Employee will be fully liable for the loss of the computer unit/laptop or its accessories/peripherals regardless of when, where or how these were lost. This will be covered by Property Accountability Form as documented in the Asset Management Policy.
- 5.1.3. Employee may access, use or share the company's proprietary information only to the extent it is authorized and necessary to fulfill the assigned job duties.
- 5.1.4. The employee has full accountability for upkeep of the computer unit/laptop and responsible for exercising and employing necessary security control to ensure the protection of the computer unit/laptops and all information stored on it.
- 5.1.5. Any employee that has computer unit/laptop security maintenance related concern should be directly reported to the Information Technology Department. Refer to Information Security Workstation Policy.
- 5.1.6. Users not limited to employees must comply with the company's password related policy. Refer to Password Policy.
- 5.1.7. Users must not use the same password that he/she uses to access his/her personal accounts thru web sites to access company IT resources. Refer to Password Policy.
- 5.1.8. Employees are accountable for ensuring that the latest antivirus definitions on the computer. This also covers client machines accessing the wireless network.
- 5.1.9. For security and network maintenance purposes, authorized individuals within the company may monitor equipment, systems, and network traffic at any time.
- 5.1.10. Intellicare Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with the policy.
- 5.1.11. Intellicare Group reserves the right to monitor and/or search any part of its computer or communications resources at any time and for any reason. With this, employees should

not consider things like computer discs, computer programs, computer journal entries, e-mail, voicemail or any other electronic communication to be private.

- 5.1.12. Company owned devices such as laptop, camera, flash drive, mobile phones, and external storage intended are for Business Use Only.
- 5.1.13. Information brought into such services and devices through the internet or other communications networks is proprietary and confidential. Employees may not copy, transfer, transmit, or otherwise share corporate information to external individuals or parties without the consent and approval of the owner of the information/document and their immediate head.
- 5.1.14. Any additional software (in-house or third-party) that is not part of the default software list will be requested through the software request form and must be approved by the requesting department's immediate head and must be tested and reviewed for possible vulnerabilities by IT Security Team and ERCMD.
- 5.1.15. Use of file sharing sites must be limited to the allowed tool and application of Intellicare Group. File sharing sites as required by clients must be limited to SFTP and must be evaluated to ensure security controls are implemented.
- 5.1.16. Unauthorized recording not limited to video and voice is prohibited. Consent and approval of the meetings attendees must be solicited before recording.
- 5.1.17. Visitors or Third parties should also adhere to the Acceptable Use Policy for Visitors.
Refer to Exhibit B. User Acknowledgement Form for Third-Party/Visitors

5.2. Workstation Policy

- 5.2.1. Physical access on workstations is restricted only to authorized personnel.
- 5.2.2. Users shall never leave their workstations unattended, even briefly, user must logoff/lock their workstations to prevent unauthorized access.
- 5.2.3. Ensure that password-protected screen saver is enabled with a 10 - 15 minutes time-out period to ensure that workstations that were left unattended will be protected.
- 5.2.4. Ensure to comply with all applicable password policies and procedures.
- 5.2.5. Ensure that workstations are being used strictly for business purposes only.
- 5.2.6. Installation of unauthorized software/s on workstations are strictly prohibited.
- 5.2.7. User shall keep food and drinks away from workstations in order to avoid any accidental spills.
- 5.2.8. Users must shutdown workstations by end of shift.
- 5.2.9. All workstations, regardless of ownership, must be documented and registered in departmental asset inventory.
- 5.2.10. In any event workstation breach incident, everyone must report it immediately to their immediate head and ERMCD.

5.3. Security and Proprietary Information

- 5.3.1. Only company-owned devices are allowed to connect to the internal network and must comply with the Endpoint Protection Policy and Mobile Device Management Policy.
- 5.3.2. Company's information and information systems (computers, servers, systems, and networks) shall be used for official and authorized purpose only.
- 5.3.3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature on specific set time period. Please refer to Password Policy.
- 5.3.4. Users must log off or lock the screen when the device is unattended. Please refer to Clean Desk Policy.
- 5.3.5. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- 5.3.6. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware. Emails received from suspicious email addresses and with suspicious attachments must be reported to IT Helpdesk and Incident Reporting Form.
- 5.3.7. Confidential and sensitive information contained in portable devices shall be protected using encryption and hard to guess passwords. Please refer to Information Security Encryption Policy and Password Policy.
- 5.3.8. Users must be mindful of sending confidential files. All sensitive documents must be encrypted upon sharing to external parties. Passwords for the encrypted files should be sent in separate e-mail. This is to prevent unscrupulous individuals to breach data security that may lead to financial loss of the company.
- 5.3.9. Employees shall use only the company's official email facility system embedded with official e-mail disclaimer in sending confidential and sensitive information.
- 5.3.10. Due to the danger of computer viruses, malware, and security breaches, use of any personal removable media or any personal website accounts on computers and other such equipment is not allowed except in Business Continuity Events which will require approval of immediate head, IT Security Team and ERMCD.
- 5.3.11. Company-owned devices that are being brought home must be taken good care of, keep in good working order, and secured when not in use. Utilize the equipment primarily for business purposes. Report any issues/problems to the Information Technology Department (ITD).
- 5.3.12. Use of personal-owned devices are prohibited except for Business Continuity Events. The personal-owned devices should conform to the minimum-security requirements.

5.4. Unacceptable Use

The following activities are generally prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Intellicare Group authorized to engage in any activity that is illegal under local or international law while utilizing company-owned resources.

The following activities are strictly prohibited, with no exception:

5.4.1. System and Network Activities

- a. Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar law 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 the company.
- b. 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 the company or the end user does not have an active license is strictly prohibited.
- c. Accessing data, a server or an account for any purpose other than conducting Intellicare Group business, even if you have authorized access, is prohibited.
- d. 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.
- e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- f. Users are prohibited to reveal their user account password to others or allowing others to use their account, including the supervisor or manager. This also includes family and other household members when work is being done at home.
- g. Using a company 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.
- h. Making fraudulent offers of products, items, or service originating from any Intellicare Group account.
- i. Effecting security breaches or disruptions of network communication. Security breaches include, but 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 purpose of this section, “disruption” includes, but not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- j. Port scanning or security scanning is expressly prohibited unless prior notification to IT Security Team and ERCMD is made and should only be done by authorized employees with legitimate business purposes.
- k. 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.
- l. Circumventing or bypassing any user authentication or unauthorized modifications of baseline security of any host, network or account is strictly prohibited.
- m. Only company issued networking devices and equipment are to be used in the office workstations. Personal networking devices (such as broadband access point, switches and hubs, etc.) are strictly not allowed.
- n. Tampering or making unauthorized modifications to the company standard operating system configuration is strictly prohibited.
- o. Introducing honeypots, honeynets, or similar technology on the Intellicare Group network.
- p. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).
- q. Using any programs/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.
- r. Providing information about, or lists of, Intellicare Group employees or copying of company information to removable media, sending it to parties outside Intellicare Group is prohibited unless needed for a legitimate business purpose and must be approved by Group Head and ERMCD.

5.4.2. Email and Communication Activities

When using company resources to access and use the internet, users must realize they represent the company. Wherever employees state an affiliation to the company, they must also clearly indicate that “the opinions expressed are my own and not necessarily those of the company”. Information contained within or attached to an e-mail must be treated in accordance with the Information Classification. Users are expected to treat confidential e-mail information with the same care as you would with information in any other form.

- a. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (e-mail spam).
- b. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
- c. Unauthorized use, or forging, of e-mail header information.
- d. Solicitation of e-mail for any other e-mail address, other than that of the poster’s account, with the intent to harass or to collect replies.
- e. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
- f. Use of unsolicited e-mail originating from within Intellicare Group’s networks of other internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by Intellicare Group or connected via Intellicare Group’s network.
- g. Suspected files with viruses and other malicious software being attached or sent across the network.
- h. Use of an e-mail account assigned to another individual to either send or receive messages.
- i. All forms of information exchange must be used for business purposes only. All users who take inappropriate, offensive, illegal or which jeopardizes the company’s reputation will be subject for disciplinary action. HCMD shall determine the appropriate sanction to the User/s in accordance with the company’s Code of Discipline.
- j. Download, storage, reproduction and distribution of copyrighted music (audio), movies (video), games, pornographic and sexually explicit materials through local drives and network shares.
- k. Postings the same or similar non-business-related messages to large numbers of Usenet newsgroup (newsgroup spam).
- l. Downloading, transferring or any form of copying of any business and client’s documents and/or information to personal-owned devices from e-mail or sharepoint.
- m. Vigilant to catch e-mails that malware or phishing attempts. Employees shall:
 - Avoid opening attachments and clicking links when content is not adequately explained.
 - Be suspicious of clickbait titles.
 - Check e-mail and names of unknown senders to ensure they are legitimate.

- Look for inconsistencies or style red flags (i.e., grammar mistakes, capital letters, excessive number of exclamation marks).

5.4.3. Internet Access

- a. Visit sites that are applicable to line of work. Websites that fall under categories such as Games, MP3, Gambling, Nudity and Sex, and Social Networking are prohibited.
- b. Other ways of accessing the internet, such as dial-up or wireless broadband connections to an internet provider, are prohibited.
- c. Sending of unencrypted Intellicare Group's confidential and sensitive information over the internet.
- d. Using internet to commit fraud or illegal acts is strictly prohibited.
- e. Using internet for non-work-related during office hours is strictly prohibited.
- f. Use of the company's internet facility to access or download material from the internet which is unsuitable, offensive, prohibited, or which can put the company's security at risk. All internet use must be for business related purposes. HRD shall determine the appropriate sanction to the User/s in accordance with the company's code of conduct and discipline.
- g. All internet data that is composed, transmitted and/or received by the company's computer systems are considered to belong to Intellicare Group and is recognized as part of its official data. It is therefore subject to disclose for legal reasons or to other appropriate third parties.
- h. The equipment, services and technology used to access the internet are property of the company and the company reserves the right to monitor internet traffic and monitor and access data that is composed, sent, or received through its online connections.
- i. Refrain from using public e fidelity (WiFi) to access any company related sites or account.

5.4.4. Wireless Network

- a. Client devices accessing the wireless network without any anti-virus software or up-to-date anti-virus data definition.
- b. Bypassing wireless connections that did not go through a web proxy server, web monitoring and filtering software (if applicable).
- c. Company-issued pocket WiFi shall not be utilized for personal usage and outside office hours.
- d. Mobile hotspot shall not be used when supposed connected to the company network via Local Area Network (LAN).

- e. Hacking authentication to gain access to wireless network.

5.4.5. Copyright and Licensing

- a. 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 the company.
- b. Unauthorized copying of copyrighted material including, but not limited to, downloading or digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted games, music, movies, pornographic and sexually explicit objects and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.
- c. Licenses must not be uninstalled from one user’s machine and re-install on another user’s machine without written request/permission from the requesting department and approval from the immediate head or even the management.
- d. All software and documentation releases or versions that have been replaced by newer versions must be consolidated and archived for future references.
- e. Software/Program manuals must be issued to departments who requested for the software/program and must be updated following the procedure on the Section 5.3.7d.
- f. All software requests and purchases must conform with the Purchasing Policy published by Facilities and Property Administration Department. Thus, these shall be requested and approved by the Management before proceeding to plan for the software logistics and procurement.
- g. Introduction of unlicensed software to the company network may only be allowed during the Proof-of-Concept phase of purchasing, provided, the unlicensed software shall be initially accessed by the IT Security Team and ERMCD for any security concern before installation and as much possible be installed in a testing separate environment. Encompassing requirements are referred in the Purchasing Policy.
- h. Free Software (freeware), or software that can be used without incurring any costs must not be installed on company devices and utilized for any business purposes unless assessed by the IT Security Team and ERMCD for any security concern.
- i. Licenses must be registered under the company’s name not in the name of an individual end-user.

5.5. **Clear Desk, Clean Workplace, and Clear Screen Policy**

To maintain Intellicare Group’s information security commitments and objectives, the company has established minimum requirements for clean desk and clean workspace to ensure that

sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secured in locked areas and out of sight. The Clean Desk policy is not only ISO compliant, but is also part of standard basic privacy controls and company measures for a healthy and safe working environment. Thus, the following policies shall be adhered to:

- 5.5.1. Users shall be held accountable for all the activities of their workstations whether or not the user was present at the time.
 - 5.5.2. Only equipment, office supplies and documents which are necessary in the accomplishment of the day-to-day task shall be on the desktop.
 - 5.5.3. Personal belongings shall be properly kept in the mobile pedestal or locker. (ex. Bags, shoes, grooming kits, lunch kits, personal mobile phones, speakers, headsets, radios and the like). These items may be taken out only during official break time.
 - 5.5.4. System units must be locked when workspace is unoccupied or unattended even for a short period of time:
 - 5.5.4.1. Technical security controls for idle time/inactivity shall be implemented for 10-15 minutes;
 - 5.5.4.2. Manual locking of screens by pressing the Windows Key W and L shall be done by the user
- This ensures that the contents of the computer are protected from the prying eyes and the computer is protected from any unauthorized use. Computers left unattended provide the opportunity for malicious data input, modification, or deletion, often with a negative consequence to the actual employee.
- 5.5.5. Passwords shall not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
 - 5.5.6. All printers and fax machines should be cleared of papers as soon as they are printed and employees shall ensure that sensitive documents are not left in printer trays for the wrong person to pick up.
 - 5.5.7. Whiteboards containing restricted and/or sensitive information should be erased at the end of each discussion to avoid disclosure to unauthorized individuals.
 - 5.5.8. Notes or pictures shall not be posted on computer monitors, modular partitions, corkboard, or bulletin board. Only official memos and announcements shall be allowed on cork boards and bulletin boards.
 - 5.5.9. Classified information must not be left unattended on or around the workstation. Papers and computer media containing classified information must be stored safely when not in use.
 - 5.5.10. Employees shall ensure that all Intellicare Group confidential information they handle, either in hard copy or electronic form, are secured in their workstation at the end of the day and when they are expected to be gone for an extended period.
 - 5.5.11. Physical documents containing Personal Identifiable Information, and Confidential Information must be kept in locked pedestal, locked cabinets, or locked storage rooms at all times unless currently in use.

- 5.5.12. Filing cabinets, pedestal, and storage rooms containing classified information must be locked when not in use and when not attended.
- 5.5.13. Portable computing devices such as laptops, tablets, and mobile phones as well as mass storages including CDROM, DVD, or USB drives must be locked away in a drawer or be locked with a locking cable, if applicable.
- 5.5.14. At the end of business day, there shall be no documents left on the employee's workstation and everything should be kept and arranged.
- 5.5.15. When disposing Intellicare Group physical documents containing Confidential and Protected Health Information, the documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins. Cross-cut shredding is recommended for Intellicare Group confidential information.
- 5.5.16. Employees must also observe these controls to maintain a healthy and safe environment in the office premises:
 - 5.5.16.1. Perishable goods shall not be stored or left in the mobile pedestal after each working day to prevent the infestation of insects/rodents.
 - 5.5.16.2. For special occasions like birthdays, personal decorations shall be minimized to prevent cluttering in the employee's workspace. Personalized greetings shall be allowed only on the day of the occasion and shall be cleared the following day.

5.6. Reporting

- 5.6.1. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of Intellicare Group proprietary information within two (2) hours from knowledge. Risk owners shall be responsible of reporting such event and must refer with the documented procedure under Incident Reporting Policy.
- 5.6.2. Employees should immediately notify their department head of any actual or suspected unauthorized use of their assets, email or any other breach of security.
- 5.6.3. Intellicare Group employees who are required and have access to the company's information or information systems, company equipment, workstations, peripherals, information media and communications infrastructure must indicate the acceptance to the company's information systems Acceptable Use Policy and other policies associated with this access. This indication is evidenced by signing the acknowledgement form. ***Refer to Exhibit A. – User Acknowledgement Form for Employees***

5.7. Third-Party/Visitors General Use and Ownership

5.7.1. Acceptable Use

- 5.7.1.1. Third-party/ is/are given use of the company's network systems in order to carry out a specific job for the company.

- 5.7.1.2. Third-party/visitor shall comply with the company's system security and not disclose any passwords provided by the company's administrators or other related authorities.
- 5.7.1.3. Third-party/visitor shall not browse, download, upload, or distribute any material that could be considered offensive, illegal, or discriminatory whilst using the company's network.
- 5.7.1.4. Third-party/visitor understands that all use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Information Security Office.

5.7.2. Unacceptable Use

The following activities are strictly prohibited, with no exceptions:

- 5.7.2.1. Accessing information, a server or an account for any purpose other than conducting Intellicare Group's business, even if you have authorized access, is prohibited.
- 5.7.2.2. Introduction of malicious programs into the network via workstation, server, peripherals or any removable devices (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
- 5.7.2.3. Revealing your account password or any user accounts to others or allowing use of your account by others.
- 5.7.2.4. Using a company asset to actively support illegal activities, and procuring or transmitting material that is in violation against harassment or hostile workplace laws in the user's local jurisdiction.
- 5.7.2.5. Effecting security breaches or disruptions of network communication. Security breaches include, but not are limited to, accessing data of which the employee's/third-party is not an intended recipient or logging into a server or account that 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 overwhelming the victim the series of PING command until he reaches denial-of-service (DoS), packet spoofing or impersonating a data to hide the actual source and DoS which is an interruption to access the workstations and servers because of malicious intent.
- 5.7.2.6. Port scanning or security scanning is expressly prohibited unless prior notification to IT Security Team and ERCMD is made and should only be done by authorized third-party personnel with legitimate business purposes.
- 5.7.2.7. Executing any forms of network monitoring which will capture data not intended for the third-party host, unless this activity is a part of the normal job/duty.

- 5.7.2.8. Bypassing user's identity verification or security of any workstation, network or account.
- 5.7.2.9. 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.
- 5.7.2.10. Bringing any unapproved devices such as mobile phone, tablet, laptop, and desktop to access the company resources, data and system is strictly prohibited.
- 5.7.2.11. Material or content accessible through the company's network may be subject to protection under laws pertaining to privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights, patents, trademarks, trade secrets or other intellectual property. Users shall not use the company's network in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

5.7.3. **Acknowledgement of Use**

- 5.7.3.1. Each third-party/visitors shall acknowledge that they have read and agreed to the Acceptable Use Policy (for third-party/visitor) when using computer, network and other electronic resources owned, leased, or operated by Intellicare Group. Signing the Exhibit B – User Acknowledgement Form for Third-Party/Visitors signifies that they understand that non-compliance and disregarding any of the AUP provisions, will be reported to their employer and that legal action may be taken and initiated against them.
- 5.7.3.2. The AUP User Acknowledgement Form may form part of the Vendor Non-Disclosure Agreement and/or Master Vendor Service Agreement during the vendor onboarding process.
- 5.7.3.3. Individuals visiting a department for official business purposes that requires access to information assets and systems of Intellicare Group must sign the Exhibit B – User Acknowledgement Form for Third-Party/Visitors. The department head hosting or accepting the visitor must provide the Form and ensure that this is accomplished prior accessing Intellicare Group information assets.

6. **POLICY COMPLIANCE**

The ERMCD will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

An employee found to have violated this policy may be subject for disciplinary action, up to including termination of employment, in accordance to the Intellicare Group's Code of Discipline.

7. **POLICY EXCEPTIONS**

Any exception to the policy must be reviewed, assessed, and approved by Enterprise Risk Management Compliance Department (ERMCD) in advance.

Any exceptions to the policy must be documented and agreed to by the approving authority.

8. POLICY AWARENESS

The Acceptable Use Policy shall be communicated to all employees of Intellicare Group through various methods including the AUP User Acknowledgement Form, e-Learning program, Information Security Advisory, Memorandum and other mediums.

The AUP User Acknowledgement Form for Employees shall be cascaded to employees during the onboarding, and annually if the Policy were subjected to significant changes.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
BYJEM-JF9HH-HUTSQ-BJYDG

DOCUMENT COMPLETED BY ALL PARTIES ON
05 MAR 2025 02:13:54 UTC

SIGNER

TIMESTAMP

SIGNATURE


DESIREE ALIBIO

EMAIL
DESIREE.ALIBIO@INTELLICARE.COM.PH

SENT
05 MAR 2025 01:54:09 UTC

VIEWED
05 MAR 2025 01:55:11 UTC

SIGNED
05 MAR 2025 01:55:49 UTC



IP ADDRESS
136.158.49.61

LOCATION
BACOR, PHILIPPINES

RECIPIENT VERIFICATION

EMAIL VERIFIED
05 MAR 2025 01:55:11 UTC


JEREMY MATTI

EMAIL
JEREMY.MATTI@INTELLICARE.COM.PH

SENT
05 MAR 2025 01:54:09 UTC

VIEWED
05 MAR 2025 02:05:13 UTC

SIGNED
05 MAR 2025 02:13:54 UTC



IP ADDRESS
124.217.51.99

LOCATION
CALAMBA, PHILIPPINES

RECIPIENT VERIFICATION

EMAIL VERIFIED
05 MAR 2025 02:05:13 UTC

