


|                        |  |   |
|------------------------|--|---|
| <b>Category:</b>       | Workplace  | <b>INCA Community Services<br/>Personnel Policy</b>  |
| <b>Sub Category:</b>   | Technology Resources   |   |
| <b>Effective Date:</b> | 06/2011  |   |
| <b>Revision Dates:</b> | 1/15, 1/17, 2/18, 1/19,<br>1/20, 1/21,1/22   |   |
| <b>Forms:</b>          |  |   |
| <b>Responsible:</b>    | Management Members,<br>Program Directors, Executive<br>Director, Human Resource<br>Manager |   |

## Computer/Internet/Email Policy

### Purpose/Introduction

Computer information systems and networks are an integral part of business at INCA. This policy and directives have been established in order to protect this investment, safeguard the information contained within these systems, and reduce agency and legal risk. Violations of this policy may result in disciplinary action in accordance with INCA's policies and procedures. Due to the ease of availability and the potential for good and/or harm, we must adopt certain very specific rules and regulations for computers, internet, and email.

### Policy

It is INCA's policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. All employees should be aware that anything they access on their work computer/laptop/tablet/other device belonging to the agency, the agency's internet access, personal or agency emails are subject to the guidelines written within. Personal cell phones/tablets/devices may also be subject to this policy. A Barracuda filter is utilized to ensure protections are in place for all computers and networking systems.

### Guiding Principles

The agency trusts and expects employees to exercise personal responsibility whenever they use the agency's computers, Internet, or email or social media accounts, which includes not violating the trust of those with whom they are engaging. Employees may use social media to speak for themselves individually or to exercise their legal rights. If there are misrepresentations made by the media, analysts, bloggers or other social media users a designated employee will be assigned by the Executive Director to respond to the issues. Do not break confidentiality in any way to defend the agency. Employees are responsible for making sure that their online activities do not interfere with their ability to fulfill their job requirements or their commitments to their managers, co-workers or customers.

### Policy General Guidelines

- Employees do not have a personal privacy right regarding any matter created, received, stored or sent from/on the agency's email, Internet system, or computers.
- The agency reserves the right to inspect and disclose the contents of any individual's agency email account, but will do so only when it is deemed necessary by the Program Director or the Executive Director.
- The agency reserves the right to disclose any agency email correspondence to law enforcement officials, without notice.
- INCA's email, Internet, and computers may not be used for any purpose that is illegal, against INCA policy or contrary to INCA's best interest.
- Solicitation of non-INCA business or any use of INCA agency email, Internet, or computers for personal gain is prohibited.
- Each employee is responsible for the content of all text, audio, or images that he or she places on or sends over INCA's computers, Internet, or email.
- Employees may not hide their identities or represent that any email or other electronic form of communication was sent from someone else or someone from outside of the agency.
- If you produce, collect and/or process business-related information in the course of your work, the information remains the property of INCA. This includes such information stored on third-party websites such as webmail service providers.
- All communications sent by employees through INCA's Internet, or email, must comply with all INCA policies and may not disclose any confidential information.
- The employee should notify his/her supervisor immediately if any unsolicited email received from outside INCA appears to violate this policy.
- If any employee accidentally accesses an inappropriate website in the normal course of business, the employee should notify his or her supervisor immediately.
- The agency maintains the right to monitor the volume of Internet and networking traffic. The specific content of any transactions will not be monitored unless there is a suspicion of improper usage.
- Employees should refrain from using personal email accounts for agency business.
  - If an employee is using a personal email account to handle agency business this becomes the property of the agency and could be subject to the terms listed within this policy.
- Passwords whether private or agency may be obtained through INCA's IT specialist if the accounts are accessed using INCA's Internet or network system or in the event that it becomes critical to legal or agency business.

## **Computer/Network**

Computers and network systems provide access to resources that are vital to the agency's daily operations. Usage of these tools should support the basic missions of INCA. Employees are responsible to properly use and protect information resources and to respect the rights of others. All data stored on the agency's computers belongs to the agency. Personal data can be viewed at any time by supervisors or agency IT specialists.

## **Computer/Network Guidelines**

- Critical computer equipment, e.g., file services, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided to protect electronic equipment.

- Employees will be responsible for protecting the information located on their computers and all confidential information will be kept secure.
- Employees may not use work computers or the network system to violate any rules in INCA's policies and procedures manual.
- No employee may download additional software from the Internet without prior authorization.
- Employees will not knowingly introduce a computer virus into company computers nor load diskettes or executable files unless approved by the IT representative. Any employee who suspects that his/her workstation has been infected by a virus shall immediately notify their supervisor and the IT specialist.
- Tickets in the form of an email are to be sent to the IT Specialist and the direct supervisor with any issues or concerns that need to be addressed using [support@intelligentit.pro](mailto:support@intelligentit.pro)

### **Internet/Email**

INCA encourages the use of the Internet and email because it makes communication more efficient and effective. Occasional and reasonable personal use of INCA's Internet and email services are permitted; however, Internet service and email are INCA's property. Every employee has a responsibility to maintain and enhance INCA's public image and to use INCA email and Internet access in a productive manner.

### **Internet/Email Guidelines**

- Email and Internet access may not be used for transmitting, retrieving, or storing any communications of a discriminatory or harassing nature or that are obscene or x-rated. Harassment of any kind is prohibited.
- Messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual orientation may not be transmitted or forwarded using the INCA system.
- Email messages should be composed in a way that is professional, business-like, and in good taste. You should compose email messages with the same care as hard copy correspondence.
- Abusive, profane, or offensive language may not be transmitted through INCA's network.
- An employee may not access another employee's email without the employee's permission.
- Agency email passwords may be changed by the designated representatives at any time if it is vital to legal or business relations.

### **Copyrights and License Agreements**

INCA's policy is to comply with all laws regarding intellectual property. INCA and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U.S. Code) and all proprietary software license agreements. Noncompliance can expose INCA and the responsible employee(s) to civil and/or criminal penalties. All installed software must be licensed according to the instructions of the software manufacturer.

### **Internet Safety Policy**

INCA's policy is to prevent user access over its computer network to, or transmission of, inappropriate material via Internet, email, or any other form of direct electronic communications and to prevent unauthorized access and other unlawful online activity, to prevent unauthorized online disclosure, use or dissemination of personal identification information of minors; and

comply with the Children's Internet Protection Act (CIPA). Access to inappropriate material is restricted through technology protection measures that block or filter Internet.

It is all staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyberbullying awareness and response.

### **Responsibility**

This policy applies to all agency employees, temporary employees, volunteers, contract labor, clients and visitors while utilizing agency property. Each employee shall be responsible for all computer transactions that are made with his/her User ID and password, and should adhere to procedures developed by the agency. Employees who are believed to have violated this policy will receive disciplinary action ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

### **Definitions/Acronyms**

**IT** - Information Technology

**Business Email** - Email account provided by a department mail system or approved external mailbox that is used for official agency business.

**Children's Internet Protection Act** - Pub. L. No. 106-554 and 47 USC 254(h) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet.

**Technology Protection Measure** - a specific technology that blocks or filters Internet access to visual depictions that are obscene, harmful to minors, or is of sexual content.

**User ID** - employee's identification used to log into websites and computers.

### **Dissemination of Policy**

The policy will be made available to all employees through the agency's website. The agency will educate and train employees and supervisors regarding the policy and any conduct that could constitute a violation of the policy.