INFORMATION TECHNOLOGY AND NETWORK POLICIES WITH GUIDELINES FOR RESPONSIBLE USE OF IT RESOURCES

POLICY STATEMENT

IT and Network Policies are created and mandatory to implement for maintaining, securing and ensuring legal and appropriate use of OFAA IT resources. The policy terms assures a campus community with a high quality, trusted and secure computing environment, with a responsibility of protecting and securing its property interests, data and intellectual property.

The OFAA requires people to use its information technology resources in a responsible manner, abiding by all applicable laws, policies, and regulations.

REASON FOR POLICY

The OFAA provides information technology resources to a large and diverse group, including faculty, staff, students, and guests. All members of this community are responsible for using these resources in an ethical and respectful manner that protects. OFAA's sensitive information and follows the IT policies. The OFAA must uphold the tenets of academic freedom, while recognizing that protecting information technology and data requires community members to act responsibly when using these resources.

SCOPE

This policy applies to everyone who uses OFAA IT resources, whether physically located on campus or remotely connected. Hence this policy applies to all electronic information stored or transmitted on the OFAA Network and the supporting IT infrastructure and cover all students, faculty, staff – whosoever use the OFAA network.

ENTITIES AFFECTED BY THIS POLICY

All Departments and units of the OFAA.

WHO SHOULD READ THIS POLICY

All members of the OFAA community.

INTRODUCTION

All employees and students are provided access to the OFAA computer network and the Internet. The policy on the IT infrastructure aims to regulate its use by all its authenticated users and the respectable guests. Thus everyone use it appropriately and lawfully for the continuous availability of network and Internet access.

The policy when implemented and followed ensures that the electronic information is provided to maintain and uphold the OFAA business and its mission of education, research and service.

The Priorities for the IT resources can be established and enforced when demand for computing resources exceeds available capacity. For use of OFAA - wide computing resources various priorities are:

Maximum: Uses that directly support the educational, research and service missions of the OFAA.

Lowest: Uses that indirectly benefit the education, research and service missions of the OFAA; reasonable and personal communications.

Prohibited: Amusement activities (game playing, e-trading, E-shopping, social networking, movies and songs, chatting/video chatting or use of VoIP services (like skype etc) unless permitted, use of Torrent and p2p software and all activities in violation of the Indian IT Act.

The OFAA enforces these priorities when one such usage disturbs or impacts on other more important usages.

PERSONAL RESPONSIBILITY

You agree to abide by the policy terms, by accepting your account password and related information and accessing network or Internet system.

The following are major responsibilities each party has in connection with this policy:

Department: Implement operational, physical, and technical controls for access, use, transmission, and disposal of OFAA data in compliance with all privacy and security policies, procedures, and guidelines.

User: Use all (IT) resources and data in a manner that is legal, ethical, and consistent with the mission of education, research. Abide by all applicable IT policies.

OFAA IT Office: Interpret this policy, and provide clarification and education.

TERM OF PERMITTED USE

Network and Internet access extends throughout the term of one's employment or stay at the OFAA, provided they do not violate the policy.

“The OFAA has the right to suspend the access to its IT resources and related services, at any time for technical reasons, policy violations, or other concerns.”

Internet facility can be accessed by the faculty and staff members using lan / wifi connectivity. Every faculty/Staff cabin has been provided with cabled network and it is expected that faculty/Staff members to use cabled network as preferred network.

Access to internet facility for OFAA hostel is free and is governed by rules and regulations of this policy, however access to social networking and YouTube is allowed from 3:30 PM to 8:00 AM.

Internet access can be granted to guests on demand of concerned faculty/staff members.

PURPOSE AND USE

OFAA offers access to its network and Internet facility for educational and research purposes only. If one is unsure of the business activity use whether appropriate or not, must consult the server room staff for usage.

GENERAL RULES

All users must comply with OFAA Rules, Regulations and Policies, cyber laws, IT Act of Government of India and the terms of (applicable) contracts including software licenses while using OFAA IT resources. It may include but not limited to: privacy, copyright, trademark, obscenity and child pornography; hacking, cracking and similar activities, Scams and pyramid schemes, the OFAA’s Student Code of Conduct etc.

Users are responsible for ascertaining the necessary authorizations before using the OFAA IT resources. They are responsible for the activities from their accounts. Under any circumstances, Accounts and passwords must not be used by persons other than those to whom they have been assigned by the account administrator. Any detect/suspect of unauthorized use of accounts or resources must be reported to the appropriate account administrator.

Users who violate this policy will be subjected to disciplinary action.

NETIQUETTE RULES

Employees/students must follow the rules of network etiquette (netiquette). That is, they must be polite, follow the organization's electronic writing and content guidelines, and use the network and Internet facility legally and appropriately. The OFAA will determine of the materials, files, information, software, communications, and other contents and activities that are permitted or prohibited, outlined below under violations.

VIOLATIONS

The following activities are considered as violations under The OFAA - computer network and Internet use policy (this list is illustrative, not exhaustive and may include more related activities):

Illegal activities under local, state and National laws

Any activity that is illegal is a violation of OFAA IT policy. Alleged violations will be referred to the campus Judicial Administrator. In addition, offenders may be investigated and/or prosecuted by the appropriate local, state or national authorities.

- Using, transmitting, viewing or searching for obscene and pornographic materials.
- Conducting unauthorized business on Internet (including share trading).
- Seeking inappropriate, offensive, vulgar, suggestive, abusive, harassing, belligerent, threatening, defamatory actions or misleading language and materials.
- Revealing other persons personal information, or accessing, transmitting, receiving or seeking unauthorized and confidential information.
- Making availability of any materials, whose possession or distribution is illegal.
- Circulating/Broadcasting hate mails, message/announcements or images intended to harm or humiliate others, discrimination or individual attacks on others, or expressing animus towards any person or group by any reason (contest, color, religion, national origin, gender, sexual orientation or disability) is prohibited.

Unauthorized access

Computer Systems can have security holes or other breakpoints /weak points that people can use to gain unauthorized access to the system and data. So, unacceptable and unauthorized use of IT resources and data includes (but not limited to) the following:

- Any attempt to acquire or using passwords of others; attempt to use or using the computer accounts of others;
- Accessing others folders, files, work, network (unless permitted), or computer, and interrupting communications of others.
- Any kind of transmit/Download of copyright materials without having consent from the copyright holder; one should assume all materials are confined to copyright laws except any explicit authorization to use them is provided.
- Use of social networking sites unless permitted.
- Watching/downloading movies and songs.
- Making OFAA IT resources available to individuals not related to OFAA without approval of an authorized OFAA official.
- The interception of communications by parties not explicitly intended to receive them without approval of an authorized OFAA official.
- Unauthorized duplicity or use of licensed computer software.
- Any unauthorized access, control, or broadcast of electronic information or data that is confidential under the OFAA's policies.
- Connecting your machine to any wireless network other than the designated network while on-campus, unless authorized.
- Providing substances prohibited by the universities employment policy/IPR Policy or the Employee Rules regulations.
- Any attempt to alter any OFAA computing or networking resources without taking permission or beyond individual's level of authorization; Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services.

- Maliciously accessing, altering, deleting, damaging or destroying any computer system, network, program or data. Examples are:
    - Changing or deleting another user's account/password of another user,
    - Using an unauthorized account, damaging or deleting OFAA files
    - Altering the OFAA network system, mishandling, damaging or tampering with computer equipment, software or settings.

Mailing Violations

Flooding someone with numerous/ large e-mails or with suspicious content is to disrupt them or the related group, which causes problems not only for the local system but also disrupts service for thousands of other innocent bystanders. Such activities include, but are not limited to, the following:

- Using the OFAA e-mail system to relay personal e-mails.
- Engaging in spam activities (i.e., sending unsolicited electronic communications to large groups of individuals at the same time) or sending e-mail chain letters.
- Sending hate mail, statements or images intended to injure or humiliate others, threats, personal attacks on others or statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability is prohibited. This includes any such messages transmitted via e-mail, instant messaging or any other electronic means which rely on the OFAA network for transmission.
- Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts; Unauthorized scanning of networks for security vulnerabilities.
- Wasting the computer resources, printer toner or paper, sending electronic chain letters, e-mail copies to nonessential readers, e-mails to group lists unless it is appropriate for everyone on a list to receive the e-mail, and organization wide e-mails without your supervisor's permission.

Forgery

- Altering electronic communications to hide your identity or to harm some other person, even ones that are intended as pranks or jokes are considered as violations. A few of them includes:
- Alteration of the content of a message originating from another person or computer with intent to deceive.
- Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication.
- Using the OFAA network or computer resources for commercial purposes or personal gain.
- Misrepresenting oneself as another user by using their ID's.

Security and Network Breach

- Installing software on any OFAA owned equipment (pirated or freeware/shareware). Using software that is not licensed or approved by THE OFAA.
- Attempting to monitor or capture OFAA network traffic.
- Intentionally compromising the privacy or security of electronic information; and intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).
- Attempting to security of various software or other security measures placed on OFAA network systems or computers.
- Creating LMS courses without content which misleads the students and OFAA members.
- Engaging in illegal activities, violating the Employee Codes/Rules/regulations, or encouraging others to do so.
- Circumventing network bandwidth restrictions by altering the network address.
- Mishandling, damaging or tampering with computer equipment, software or settings.
- Disrupting or attempting to disrupt network traffic or attempting to overload or crash the OFAA network and attached systems.
- Maintains insecure passwords on IT devices attached to the network
- Attaching misconfigured IT devices to the network.
- Compromising an IT device, use of an application or computing system attached to the network.
- To perform network or system scans on resources not authorized by the IT security department.

GUIDE LINES

1. Network registry:

OFAA is concerned with creating and maintaining a central registry service. The said service maintains an updated database with current records of all the devices connected to the central network, including the wireless connections. IT department must provide the technical tools necessary to access the central network registry service to network administrators who manage subnets.

Users and system Administration (must entries): MAC Address, IP Address (if static), Network id/user id.

Network administration:

To register all devices connected to networks under their domains for which individual users or systems administrators

Network administrators of separated subnets, must also update the network registry service with logs of addresses of devices that connect to their networks.

2. Authentication to IT resources

To protect the IT resources from unauthorized use, OFAA must protect them and support regulations governing the privacy and security of sensitive data by the use of electronic identifiers and secure passwords to control access. There are four categories of users: Applicant IDs, Net IDs or specific user IDs, Guest IDs,

Sponsored Net IDs.

Administration job:

- Passwords must be in encrypted form.
- Passwords must never be stored in clear text on a server. o Server must be in a secure area with limited access.
- System administration must be handled by some OFAA IT staff member only.
- Server should adhere to standardized procedures.
- Secure IDs should be used to access the system.

To avoid unauthorized access, users (all categories) must follow specific rules for creating and using of complex passwords as:

Do's:

Choose at least eight characters, including at least three of the following four character types:

Uppercase letters
Lowercase letters
Numbers
Symbols found on your keyboard, such as ! * - () : | / ?...including blank spaces.

Don'ts:

Use words from the dictionary
Use names or nicknames, address, birthday, etc.
Include any of these:
Repeating characters, such as AAA or 555
Alphabetic sequences, such as abc or CBA
Numeric sequences, such as 123 or 321
Common keyboard sequences, such as ABCD

3. Mass E-mailing

An e-mail directed to any or all of the following: faculty, staff (academic and nonacademic), student, and alumni. There are two forms of mass e-mail communication: emergency and non-emergency.

Emergency E-mail: can be send to all except alumni. An e-mail that is distributed with max priority, above all others. It has a deleterious effect on network performance, and is therefore used only in urgent or extraordinary circumstances.

Non-Emergency E-mail: may sent to all.

Whosoever wishes to send mass e-mail must take permission from the higher administration top officials, along with the permission of staff and faculty members (which are included).

DATA BACKUP

Google drive, which is a complete Data management solution. Following steps will be adhered by all while using the Google drive.

- Download Google drive on your PC to keep files in sync with your files stored on the web.
- Desk top version can be downloaded: http://www.google.co.in/drive/download at Carry out the two-step verification for security purposes.
- This facility to be used only for Academic purpose/official documents and not for recreational/personal requirements like songs, movies, personal photographs etc.

CONFIDENTIAL INFORMATION

Employees may have access to confidential information about THE OFAA, once written approval is granted. With the approval of management, employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mail must be marked "confidential." When in doubt, does not use e-mail to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

PRIVACY

Network and Internet access is provided as a tool to accomplish the organization's strategic goals and objectives. The OFAA reserves the right to monitor, inspect, copy, review, and store at any time and without prior information any and all network and Internet use, as well as any and all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with this use. All such information, content, and files are the property of The OFAA. Network administrators may review files and intercept communications for any reason, including, but not limited to, maintaining system integrity and ensuring employees are using the system in accordance with this policy.

NONCOMPLIANCE

The use of the computer network and the Internet is a privilege, not a right. Violation of this policy, at the minimum will lead to disciplinary action. Policy breaches include violating the above provisions and failing to report violations by other users. Permitting another person to use your account or password to access the network or the Internet including, but not limited to, someone whose access has been denied or terminated is a violation of policy. In case another user violates this policy using ones account, the account holder will be held responsible and both will be subject to disciplinary/administrative action. Criminal violations may lead to criminal or civil prosecution.

SECURITY MEASURES

Physical security: to protect resources such as keys, doors, and/or rooms maintained to the level of security commensurate with the value of the resources stored in those locations.

Administrative security: to protect resources such as:

- Full implementation of the most current authentication and authorization technologies.
- Most recently tested and approved software patches available.
- Most contemporary and available security configurations.
- Most contemporary and available virus protection.
- Configuration of secure passwords on all IT devices

REVISION

This policy may be modified as deemed appropriate by the OFAA. Users are encouraged to periodically review the policy as posted on the OFAA's website page.

WAIVER

When restrictions in this policy interfere with its service mission, research, or educational, members of the OFAA community may request a written waiver from the Registrar, THE OFAA, Chennai.

CONTACTS

Employees/students can contact the server room for any information security related issue at: e-mail: info@orientflights.com

WEB ADDRESS FOR THIS POLICY

https://orientflights.com

DISCLAIMER

Security is neither perfect nor permanent. This is even more true for Information and IT infrastructure where change is the only constant - systems change, requirements change, new bugs are discovered, new vulnerabilities are disclosed, new threats arise, old vulnerabilities take new forms - all this as the information and the equipment go through their lifecycles from creation and use to destruction, and from great value for the organization to none. In this

Dynamic environment, this document attempts to bring some long-lasting order and balance. Owing to the very nature of its subject, this document, too, is neither perfect nor permanent. The document must necessarily be periodically updated for it to remain effective.