1. Purpose

The purpose of this document is to set out the policies of Cagayan State University at Andrews on the acceptable and prohibited use of its information and communication technology (ICT) facilities and the sanctions for non-compliance. The policy specifies how the University fulfills its job in maintaining functionality and good performance of the ICT resources for better delivery of services. This addresses the need to protect the data bank on university information against misuse and users' data against unauthorized access, spy wares, viruses and the like that may cause serious damage to the information system.

2. Scope and Definition

2.1. The CSU Andrews ICT facilities are provided and managed by the University Planning and Development Office (UPDO) through its Management Information Service (MIS) and are made available primarily for the purpose of providing authorized users in supporting learning, teaching, research, administration, and approved business activities of the University.

2.2. This set of rules apply to all authorized users--administrators, administrative staff, faculty members, students, alumni, officials, partners, contractors, third parties, and guests--who use the central administration local area network (LAN) or any of its components. An authorized user is a person who has been provided access to the University ICT facilities.

2.3. ICT facilities encompass (but not restricted to) the following resources and services provided by the University and third parties on its behalf:

a. network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with the network servers, firewall, connections, switches and routers;

b. network services, including (but not exclusively) internet access, web services, email, wireless (wifi), messaging, shared file storage, printing, telephony and fax services, and CCTV;

c. university owned or leased computing hardware, both fixed and portable, including (but not exclusively) desktop computers, laptops, tablets, PDAs, mobile devices, smartphones, servers, printers, scanners, disc drives, monitors, keyboards and pointing devices; and

d. software and databases, including applications and information systems, virtual learning and videoconferencing environments, ICT laboratories, information services, e-journals and e-books.

2.4. The ICT facilities available will vary per user group/office; some users will only be entitled to use some limited facilities.

2.5. The University may introduce changes to the Policy at any time. Users will be informed of the changes done in the widest possible means.

3. **Policy Statements**

3.1. Any individual using the ICT facilities of the University is deemed to have accepted the policy and is bound by it.

3.2. The use of the University ICT facilities is not a right, but a privilege, which can be taken away by the management once authorized users are not complying with the provisions of this policy. The University reserves the right to take appropriate action against individuals using, or suspected of using, its ICT facilities in a manner they decide is unacceptable.

3.3. The University allows reasonable personal (occasional and limited) use of ICT facilities by authorized users, subject to the discretionary limits identified in this policy. The University's business purposes of ICT facilities take priority consideration over any personal use.

4. **Acceptable Use**

All authorized users of the ICT facilities must comply with the following principles:

4.1. Each user is issued a valid user name and password which must be used to authenticate and gain access to the ICT facilities. The password must be kept confidential and must not be shared with anyone else. Access to the ICT facilities using someone else's username and password is not allowed.

4.2. All users must help maintain the reliability, availability, and efficiency of hardware and network resources

4.3. All users must update their own antivirus software everyday for the purpose of protecting own files from viruses on the net.

4.4. Always scan files from the Internet, USB, or CDs with antivirus before opening the contents. If the antivirus could not clean the infected files, immediately ask assistance from the MIS technical.

4.5. Shutdown computer immediately and report to UPDO-MIS Office if computer is infected with a computer virus.

4.6. Computer files should be regularly backed up by end user.

4.7. On regular basis, all users must store or save and update common files in the designated file server not only in their own computers.

4.8. In cases of brownouts or power outage, always shutdown the computers properly before the UPS battery runs out of power.

4.9. All programs installed in the university computers must all be licensed with the exception for freeware or Open Source.

4.10. Always log off, lock, or shutdown the computer after use.

4.11. All users should be courteous and considerate of others when using the ICT facilities.

4.12. All should ensure personal use is occasional, reasonable, and compatible with and does not contravene the primary purpose of the facilities, does not interfere with, conflict with or take priority over the performance of University duties; does not waste resources, deny or impair the service to other users or have a negative impact on the University or other users.

4.13. In case the staff is absent or on leave, his or her work communications and other files may be accessed during his or her absence but such access will only proceed if request is granted by the UPDO-MIS Director.

4.14. All should get appropriate authorization before sending or transmitting University confidential information.

4.15. Users should utilize good information security and management practices for storage, access, retention, and deletion of University information.

4.16. Users should obtain authorization/clearance from UPDO-MIS for purchasing/obtaining software licenses and for installing on CSU-owned computers.

4.17. Procurement of computer hardware such as laptop, and desktop computers must comply with the specification standards set by the UPDO-MIS.

4.18. When desktop computing equipment is required to be moved from one location to another or when the equipment is temporarily setup in another location, staff must submit their request to the UPDO-MIS for technical assistance. This will enable the UPDO-MIS to ensure that the equipment is working correctly after the move is completed.

4.19. All should make necessary efforts to send data that is virus free and not open email attachments or click on links sent by unsolicited or untrusted sources.

4.20. Users will be solely responsible for claims, liabilities, damages, costs and expenses suffered or incurred by the University which result from their use of the ICT facilities in contravention of this policy.

4.21. Submit an appropriate request to the UPDO-MIS when seeking for copies of CCTV footages/clips for authorized use.

4.22. Users should report any technical problems, requests or concerns regarding a suspected policy breach directly to UPDO-MIS.

5. **Prohibited Acts**

When using the ICT facilities, users must not:

5.1. Deliberately or unintentionally receive, access, create, change, store, download, upload, share, use or transmit any material which is

a. violent or that which glorifies violence;

b. promoting crime, terrorism, extremist activities or glorifying criminal activity (including drug abuse);

c. offensive or racist or designed to incite racial hatred;

d. of extreme political opinion;

e. pornographic or with otherwise unsuitable sexual content;

f. crude, profane or with otherwise unsuitable language;

g. blasphemous or mocking of religious and moral beliefs and values;

h. in breach of the law, including copyright law, data protection and computer use;

i. belonging to other users of ICT systems and which they do not have explicit permission to use;

j. infected or with malicious code (including, but not restricted to, computer viruses, spyware, trojan horses and worms) whether designed specifically or not, to be destructive to the correct functioning of computer systems, software, networks, data storage and others' data, or attempt to circumvent any precautions taken or prescribed to prevent such damage;

k. discriminative or encouraging discrimination on any grounds;

l. deemed by the University to be advocating, inciting or encouraging illegal activity, threatening, harassing, defamatory, bullying or disparaging of others, abusive, libelous, slanderous, indecent, obscene, offensive or otherwise causing annoyance, inconvenience or needless anxiety; and

m. infringing the copyright or confidentiality of another person or institution, or infringing the copyright law of the Philippines and/or other countries (including but not exclusive to music, films, radio and TV).

5.2. Search for, or use websites that bypass the University's internet filtering and firewall;

5.3. Download any program from the Internet that is not licensed. The exceptions include updates for Microsoft, SunJava, Adobe Flash and Adobe Reader, and Anti-virus;

5.4. Seek to gain unauthorized access into or interfering with another computer to corrupt, alter, or destroy its system;

5.5. Use other people's user ID or password even with their permission;

5.6. Interfere with or cause malicious damage to the ICT resources and facilities;

5.7. Access any University system by circumventing the network authentication process;

5.8. Obtain unauthorized commercial gain or obligations;

5.9. Carry out activities of a nature that compete with the University in business;

5.10. Sell or redistribute any part of the ICT facilities;

5.11. Carry out activities that conflict with an employee's obligations to the University as their employer;

5.12. Carry out activities that unreasonably waste staff effort or network resources or activities that unreasonably serve to deny ICT facilities to authorized users;

5.13. Carry out activities that criticize or harm individuals or that violate the privacy of other individuals;

5.14. Gain or attempt to gain unauthorized access to facilities or services via the University ICT facilities, using automated processes or otherwise;

5.15. Allow, incite, encourage or enable others to gain or attempt to gain unauthorized access to, or carry out unauthorized modification to the

University's or others' ICT facilities;

5.16. Overload, change, damage, curtail, corrupt, disrupt, deny, modify, re-route, dismantle or destroy (or cause to be overloaded, changed, damaged, curtailed, corrupted, disrupted, denied, modified, re-routed, dismantled, or destroyed) any ICT facility, network component, equipment, software or data, or its functions or settings, which is the property of the University, its Users, visitors, suppliers or anyone else, without the express permission of the UPDO-MIS;

5.17. Connect any non-approved or personally owned ICT equipment to the University physical (wired) network points without written authorization of the UPDO-MIS Director;

5.18. Save or share any University owned confidential information on any cloud computing service unless it is under a negotiated contract approved by the University;

5.19. Otherwise transmit, distribute, discuss or disclose (on message boards, email or any other mechanism) any University owned or held confidential information;

5.20. Continue to use any item of networked hardware or software after a designated UPDO-MIS authority has requested that use ceases because of its causing disruption to the correct functioning of the University ICT facilities, or for any other instance of unacceptable use;

5.21. Install, attempt to install, or store programs of any type (including screen savers and custom mice) on the computers without permission from the network administrator.

5.22. Eat or drink near computer equipment.

5.23. Configure computer settings or install any equipment without the knowledge or presence of the UPDO-MIS technical;

5.24. Open files brought in on removable media (such as CDs, flash drives, etc.) until they have been checked with antivirus software, and have been found to be clean of viruses.

5.25. Connect any mobile equipment to the network until they have been checked with antivirus software, and been found to be clean of viruses;

5.26. Bring home ICT resources without proper authorization;

5.27. Access social networking sites during normal office/working hours or classes. "Social Networking" (e.g. MySpace, Twitter, Facebook, etc.) sites are only allowed before work and during noon break on office days and on weekends when employees are authorized to do overtime.

5.28. Access to internet messengers such as AOL, Yahoo! Messenger, Chikka, Skype, and the like while at work.

5.29. Use “Peer to Peer” (e.g. Limewire, Youtube Downloader, Utorrent, Bittorrent, etc.) sites that could cause congestion of bandwidth traffic.

5.30. Play online computer games.

5.31. Access to sites such as Youtube and any other online movie or music players that eat so much bandwidth and that slow down the network.

5.32. Commit the University via means of email to a contract (except for staff who are expressly authorized to do so using University procuring procedures);

5.33. Falsify emails to make them appear to have been originated from someone else, or send anonymous messages without clear indication of the sender;

5.34. Use corporate email accounts for personal or commercial purposes;

5.35. Intentionally or unintentionally transmit unsolicited or unauthorized commercial or advertising material within the University or to other individuals or organizations in contravention of the University privacy statement or use any portion of the ICT facilities as a destination linked from such material. Such material includes unsolicited e-mail (spam), chain letters, hoax virus warnings, pyramid letters or other junk mail of any kind.

6. **Monitoring**

Management reserves the right to monitor communications.

6.1. UPDO-MIS shall employ monitoring techniques on its ICT systems and services, including e-mail and Internet access, to enable usage trends to be identified and to ensure that these facilities are not being misused.

6.2. UPDO –MIS shall keep logs of: calls made on communications equipment such as telephones and fax machine; official emails sent by e-mail addresses; internet sites visited by computer system address. In some cases, this means that the identity of the individuals involved in the communication is readily available. These logs may not be routinely monitored on a continuous basis but spot-checks are carried out from time to time to help ensure compliance with this policy. Authorized investigations may be necessary where there is reasonable suspicion of misuse of facilities.

6.3. Since the University owns and is liable for data held on its communications equipment and systems, it reserves the right, as part of any investigations, to inspect the contents of corporate (offie) e-mails or any other form of communications that are sent or received and of Internet sites accessed, for compliance with this policy. This will only be done where the volume of traffic or the amount of material being downloaded is excessive, or there are grounds to suspect that use is for ‘unacceptable’ or ‘forbidden’ activities.

6.4. Exceptionally, where there is a defined and valid reason for doing so, the inspection may include items marked ‘private’ or ‘personal’. An individual’s e-mail and voice-mail accounts may also be accessed by management when the individual is absent from work to ensure official business matters can be effectively dealt with. Authorization for such access is given by the UPDO Director or his/her official representative. Management will make a reasonable attempt to inform and obtain agreement from the user prior to this occurring.

6.5. Monitoring/investigations of individuals’ use of the University’s communications systems may also happen in the following circumstances: 1) To detect or prevent crime including detecting unauthorized use of systems, protecting against viruses and hackers and fraud investigation; 2) To assist in maintaining the security, performance, integrity and availability of the ICT systems, services and facilities, and 3)To provide evidence e.g. of a commercial transaction, to establish regulatory compliance, audit, debt recovery, dispute resolution.

6.6. Where monitoring is used, only UPDO-MIS staff trained in data protection compliance will investigate the recorded data. Confidentiality will be ensured for all investigations involving personal data, except to the extent that wider disclosure is required to follow up breaches, to comply with University orders or to facilitate investigations.

6.7. In addition, trained UPDO-MIS staff will conduct random audits on the security of the University’s ICT systems. These audits include examination of a small, randomly selected set of user devices and server systems. The audit checks that these systems have correctly licensed software, do not contain inappropriate material and have not been used to access or view inappropriate material that may violate this policy.

6.8. Where monitoring reveals instances of suspected misuse of the ICT systems (e.g. where pornography or other inappropriate material is found, or where substantial time-wasting or other unacceptable/forbidden use is found), these will be investigated through normal disciplinary procedures and may result in dismissal.

6.9. To help safeguard users’ privacy, it is suggested that employees mark any personal e-mails they send with the word ‘Private’ in the “subject” line and to ask those they correspond with to similarly mark any personal e-mails being sent. Personal files, documents and e-mails can be stored in ICT systems provided they are in a folder clearly marked as ‘Personal’ or ‘Private’. Note that corporate electronic document or record management facilities do not include a facility for personal data so should not be used for this. Where possible, those staff responsible for monitoring or inspecting the IT and communications systems will respect e-mails and folders which are marked

‘Personal’ or ‘Private’. In cases where misuse is suspected, all appropriate ICT systems, including emails and folders marked ‘Personal’ or ‘Private’, will be checked to establish whether there may be a case to answer.

At management discretion, CSU Andrews employees are allowed limited and reasonable personal use of University ICT systems, services and facilities provided that such use does not interfere with their (or others’) work; and/or involve more than minimal amounts of working time; and incur any significant expense for the University and/or tie up a significant amount of resource.

6.10. Personal use should be limited to non-working time e.g. at lunchtime, before/after normal working hours, or when “clocked out” for members of flexi schemes. Very limited, occasional personal use during normal working time will be tolerated (e.g. to respond briefly to an incoming personal e-mail or telephone call or to deal with a non-work related emergency). However, spending significant amounts of time making personal use of the internet, e-mail, communication equipment, etc. is not acceptable and may lead to disciplinary action.

7. **Sanctions**

7.1. Users who become aware of a possible breach of this policy must report to the office head, UPDO Director, Chief Administrative Officer or to the University President.

7.2. The University may take disciplinary action against anyone whose use of ICT facilities violates this policy.

7.3. Sanctions for breaches of this policy may include restricted access to ICT facilities, withdrawal of privileges to get access to ICT facilities, and possible dismissal from the service.

Cagayan State University Andrews Campus

ICT Acceptable Use Policy Agreement

I understand and agree to be bound by the conditions of the CSU Andrews ICT Acceptable Use Policy.

Full Name: ____________________________________

Office/Department: ____________________________________

Signature: ____________________________________

Date: ____________________________________