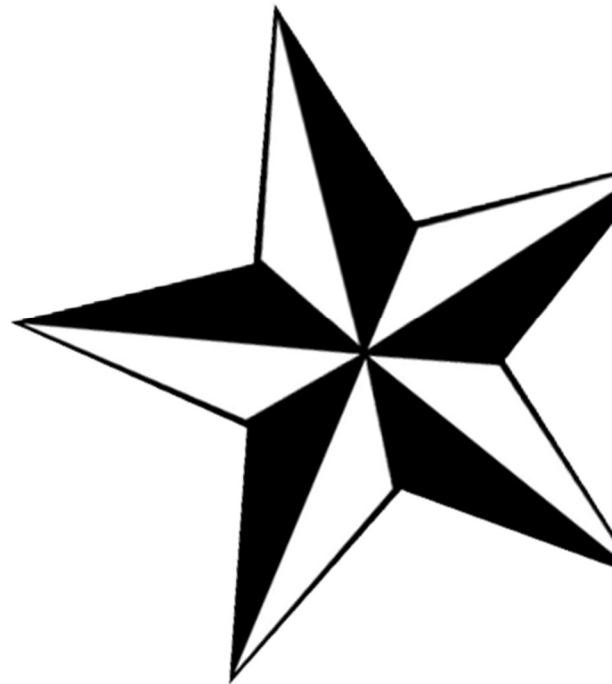




# Information and Communications Technology (ICT) Policy, Process, & Procedure Manual

DRAFT Version 1.0  
MARCH 2017





Information Technology Center  
Rm 206B Life & Science Building  
De La Salle Araneta University  
[www.dlsau.edu.ph](http://www.dlsau.edu.ph)

© 2014 by De La Salle Philippines, De La Salle Araneta University  
All Rights Reserved. No part of this manual may be reproduced in any form  
without written permission of the copyright owner.



# REVISION HISTORY

Date	Revision Particulars	Approving Authority	Effectivity Date
[MM/DD/YYYY]	REV No. 1.0	[Name of Approving Authority]	[MM/DD/YYYY]



# Acronyms & Abbreviations

DLSP – De La Salle Philippines

DLSAU – De La Salle University

ICT – Information and Communications  
Technology

ITC – Information Technology Center

SERP – School Enterprise Resource Planning



# Table of Contents

---

Table of Contents.....	iv
1. Introduction .....	1
1.1 What is the Purpose of the ICT Policies, Process and Procedures Manual?.....	1
1.2 Who are the Intended Users? .....	1
2. ITC Helpdesk Policies & Procedures.....	2
Summary of Change.....	2
3. Pull-Out Items & Return to Suppliers Policies & Procedures .....	5
Summary of Change.....	5
4. ITC Bring Your Own Device (BYOD) Policy .....	8
Summary of Change.....	8
5. Password Protection Policy .....	13
Summary of Change.....	13
6. Internet Usage Policy .....	16
Summary of Change.....	16



# 1. Introduction

---

The Information & Communications (ICT) Policy, Process and Procedure Manual provides the policies and procedures for selection and use of ICT within the institution which must be followed by all partners and students. It also provides guidelines DLSAU will use to administer these policies, with the correct procedures to follow.

DLSAU will keep all ICT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies, process and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies, processes and procedures specified in this manual are welcome.

These policies and procedures apply to all partners and students.

## 1.1 What is the Purpose of the ICT Policies, Process and Procedure Manual?

The purpose of this document is to promote a common understanding on the proper policies, processes and procedures in using and safeguarding ICT in the campus and offices for both the Administrators of the

institution, the partners and the students. Specifically, this manual seeks to:

- Ensure that all are aware of their obligations in relation to selection, use and safety when utilizing ICT within the organization.
- To help administrators make consistent and reliable decisions.
- To inform each partner and student a clear understanding as what to expect and allowed in terms of ICT.

This will bring definite and long-term benefits, reduces disputes, and adds to the professionalism of the institution.

## 1.2 Who are the Intended Users?

This document is intended for the main stakeholders of the institution – the Administrators, Partners, the ITC Department, including the students, and those who will be benefiting with the proper usage of ICT.



## 2. ITC Helpdesk Policies & Procedures

---

### Document Change Status:

Policy No./ Version No.	Date	Summary of Change
2016-1-Ver.1.0	June 2016	

Guidance: This policy should be read and carried out by all Administrators, Partners, and Personnel.

ITC Helpdesk refers to the resource intended to provide the Lasallian Partners and Students or end users with information and support related to ICT.

### 1. Purpose

This policy provides guidelines for the proper logging in and recording of service requests and event assistance pertaining to ICT and assigning of service tickets to Technical Support Specialists (TSS).

### 2. Policies

- 2.1. This policy takes into consideration the intranet app, Spiceworks used in recording, assigning and monitoring of service tickets as well as the status of the helpdesk request.
- 2.2. All ICT Helpdesk service requests must go to **<http://itc-helpdesk/portal>** using Spiceworks App and for service requests thru phone or email, they will be asked to put in a helpdesk ticket using the Spiceworks App. If the user can't, then the TSS will enter one for them.
- 2.3. Service tickets will be addressed on a first come first serve basis or in order of priority depending on the impact of the service concern within a reasonable time. Tickets will be updated with important information for the convenience of all involved.
- 2.4. The assigned TSS must confirm the completion with the user before closing it. The User or the TSS Team Leader can only close a ticket.
- 2.5. If the TSS requires a response from the ticket user, then the user will be given three attempts of contact, within a two (2) week period and update the ticket after each attempt. In the event a TSS Team Leader needs to close a ticket due to non-response, an email to the user and cc the ICT Head is needed.
- 2.6. All assigned tickets that are in "OPEN" status must be updated at least once a week on the status of the tickets.



- 2.7. In the event that a TSS does not promptly address a ticket within one (1) week, the ITC Head is notified by the TSS Team Leader and/or helpdesk manager for proper action.
- 2.8. A "CLOSED" status can be updated by the user or the TSS Team Leader ONLY for every accomplished ticket.
- 2.9. A ticket can be re-opened by the user if problem re-occur and can be assigned with the same TSS or to another by the TSS Team Leader.
- 2.10. Any user that needs ICT support for an event must create a request at least one (1) week before the date of the event. Any event that is requested less than a week before the date of the event will be supported on a "best effort" basis. In "emergency" situations, the ICT Head or Assistant Head will make the decision on which events are supported first.

### 3. Administration

The TSS Team Leader is the officer-in-charge on the administration of this policy and the implementation of processes and procedures to ensure that the needed technical assistance schedule is followed. All ICT Helpdesk requests must go to **<http://itc-helpdesk/portal>** and the officer in-charge is also authorized to:

- 3.1. Assign a Ticket with the corresponding Ticket No., assign a Technical Support Specialist and schedule the service.
- 3.2. Cancel or transfer the assigned Technical Support Specialist to another Ticket.
- 3.3. Update the status of the helpdesk request; and
- 3.4. Close a ticket.

### 4. Procedures

The following are the step-by-step procedures in requesting and addressing a service request or event ICT assistance at ITC Helpdesk:








## 5. Applicability

This policy applies to all service requests generated by Spiceworks App in the course of DLSAU's daily operations including events' ICT assistance from all the units/departments.

**NOTE: This policy can be amended/modified/withdrawn at any point in time without any notice, at the discretion of the IT Council, duly authorized by the ITC Head and approved by the President/Chancellor, De La Salle Araneta University.**

**This policy will be effective in its entirety from June 2016 and will supersede all previous circulars/communication in this regard.**

DESIGNATION		NAME	SIGNATURE
Approved by	University President, De La Salle Araneta University	Dr. Bjorn S. Santos	



### 3. Pull-Out Items & Return to Suppliers Policies & Procedures

Document Change Status:		
Policy No./ Version No.	Date	Summary of Change
2016-2-Ver.1.0	June 2016	

Guidance: This policy should be read and carried out by all Administrators, Partners, and Personnel.

Pulled-out items refer to the unrepaired ICT equipment needed to be brought to the ITC Repair Room for further check-up or repairs. If the items are still covered with the WARRANTY period, items need to be returned to the supplier for repair or replacement.

#### 1. Purpose

This policy provides guidelines for the proper pulling out of unrepaired ICT equipment to the ITC Repair Room and returning items to Suppliers for repairs. It includes proper documentation for proper monitoring and recording.

#### 2. Policies

- 2.1. This policy takes into consideration the appropriate forms needed to document the pulling out of unrepaired ICT equipment to the ITC Repair Room and returning the item/s if necessary to the Suppliers.
- 2.2. If an item is unrepairable onsite and needs to be repaired further in the ITC Repair Room, the **Pull-Out Slip (Form F-101)** should be properly filled up. The Accountable Person or User should sign to acknowledge the pull-out.
- 2.3. If the warranty of the item that needs to be repaired has already expired, the TSS in-charge should seek the approval of the ITC Head before the item would be returned to the Supplier for repair.
- 2.4. If an item needs to be returned to the Supplier or needs to be repaired outside the institution, the **Return to Supplier** portion of the slip should be filled up. The Supplier's Representative should also sign to acknowledge the receipt of the returned item/s. Properly filled up Gate Pass should also be prepared.
- 2.5. If there is a Service Charge, a **Payment Request Form (PRF)** should be accomplished by the TSS In-Charge, approved by the ICT Head, before confirming with the repair.



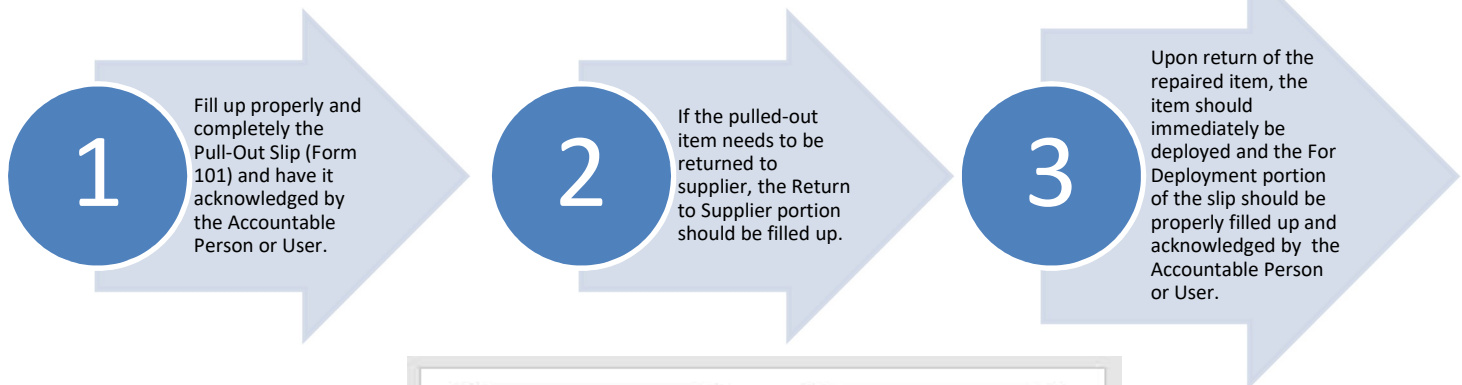
- 2.6. Upon return of the repaired item, it will be deployed immediately to the unit or department where it was pulled-out. The **For Deployment** portion should be properly filled up and the Accountable Person or User should also acknowledge the deployment.

### 3. Administration

The TSS In-Charge for Pull-Out items and Return to Suppliers should monitor and follow up the status of all the items pulled out or returned to suppliers. The TSS Team Leader is the officer-in-charge in the administration of this policy and the implementation of processes and procedures to ensure that proper documentation and monitoring is practiced.

### 4. Procedures

The following are the step-by-step procedures in pulling out items for repairs and for return to supplies:



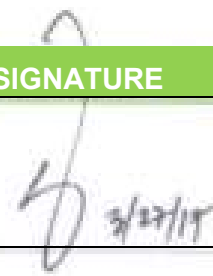


## 5. Applicability

This policy applies to all pulled-out and return to supplier items as administered by the TSS In-Charge with the approval of the TSS Team Leader.

**NOTE: This policy can be amended/modified/withdrawn at any point in time without any notice, at the discretion of the IT Council, duly authorized by the ITC Head and approved by the President/Chancellor, De La Salle Araneta University.**

This policy will be effective in its entirety from June 2016 and will supersede all previous circulars/communication in this regard.

DESIGNATION		NAME	SIGNATURE
Approved by	University President, De La Salle Araneta University	Dr. Bjorn S. Santos	



## 4. ITC Bring Your Own Device (BYOD) Policy

---

### Document Change Status:

Policy No./ Version No.	Date	Summary of Change
2017-3-Ver.1.0	March 2017	

Guidance: This policy should be read and carried out by all Administrators, Partners, Personnel, and Students.

DLSAU acknowledges the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to the institution's network and equipment. We encourage you to read this document in full and to act upon the recommendations.

### 1. Purpose

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets, phablets and other personally owned devices that will connect to DLSAU LAN and IT equipment and have access to DLSAU business apps like SERP and WebOPAC, etc. All Administrators, Partners, Personnel, including students who use or access DLSAU LAN and IT equipment including access to business apps and/or services are bound by the conditions of this Policy.

### 2. Policies

#### 2.1. Approved IT Equipment including PCs, notebooks, tablets, and mobile devices for DLSAU LAN connection and business apps use

The following personally owned mobile devices are approved to be used for DLSAU LAN connection and business apps purposes only:

- Personal Computers
- Notebooks
- Tablets
- Smart Phones or Phablets



## **2.2. Registration of Personal Mobile Devices for DLSAU LAN Connection and Business Apps Use**

Administrators, Partners, Personnel, and students when using personal devices for DLSAU's LAN connection and business apps use will register their device with the DLSAU ITC. The DLSAU ITC will provide a designated IP Address for the device and record the device and all applications used by the said device. For personal devices that only access WIFI hotspots for internet access as guests may not register anymore their devices.

However, personal devices can only be used for the following purposes:

- Internet Access for research purposes only
- Telephone/Video Calls
- Email Access
- Access to DLSAU LAN and Business Apps

Each Administrator, Partner, Personnel, or Student who utilises personal devices agrees:

- Not to download or transfer DLSAU business or personal sensitive information to the device, unless authorized. Sensitive information includes DLSAU Student Records and Personal Information, Personnel Data, Institution's Financial and Business Records, and other sensitive information of the institution.
- To make every reasonable effort to ensure that DLSAU's information is not compromised by using the said personal equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected.
- Not to share the device with other individuals to protect the business data access through the device.
- To abide by DLSAU's internet policy for appropriate use and access of internet sites, etc. (6. Internet Usage Policy, page 16 of ITC Policy, Process & Procedure Manual)



- To notify DLSAU ITC immediately within 24 hours in the event of loss or theft of the registered device to deactivate passwords and access privileges embedded on the device.

All Administrators, Partners, Personnel, or Students who have a registered personal device for business use acknowledge the following:

- To maintain the device with its assigned IP Address.
- DLSAU owns all job related intellectual property created on the device
- Will regularly back-up data held on the device
- DLSAU has first right to buy the device where the employee wants to sell the device
- DLSAU will delete all job-related data held on the device upon termination of the personnel. The terminated personnel can request personal data be reinstated from back up data
- DLSAU has the right to deregister the device for business use at any time.

### **2.3. Keeping registered devices secure**

The following must be observed when handling personal computing devices (such as notebooks, tablets and iPads):

- PCs or Mobile computer devices must never be left unattended in a public place, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended.
- Mobile devices should be carried as hand luggage when travelling by aircraft.



### **3. Exemptions**

This policy is mandatory unless the President/Chancellor grants an exemption. Any requests for exemptions from any of these directives, should be referred to the DLSAU ITC.

### **4. Breach of this policy**

Any breach of this policy will be referred to the DLSAU ITC who will review the breach and determine adequate consequences, which can include confiscation of the device and or termination of employment.

### **5. Indemnity**

DLSAU bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of personnel in accessing or using these resources or facilities. All personnel indemnify DLSAU against any and all damages, costs and expenses suffered by DLSAU arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by DLSAU.

### **6. Administration**

The DLSAU ITC is the office-in-charge on the administration of this policy and the implementation of processes and procedures to ensure that the needed technical assistance is followed.

### **7. Applicability**

This policy applies to all personally owned notebooks, smart phones, tablets, phablets and other personally owned devices that will connect to DLSAU LAN and IT equipment and have access to DLSAU business apps like SERP and WebOPAC, etc.





## 8. Compliance

### 8.1. Compliance Measurement

The DLSAU ITC will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### 8.2. Exemptions

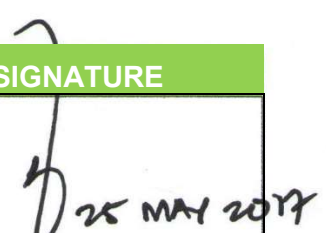
Any exception to the policy must be approved by the President/Chancellor in advance.

### 8.3. Non-Compliance

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**NOTE: This policy can be amended/modified/withdrawn at any point in time without any notice, at the discretion of the IT Council, duly authorized by the ITC Head and approved by the President/Chancellor, De La Salle Araneta University.**

**This policy will be effective in its entirety from March 2017 and will supersede all previous circulars/communication in this regard.**

DESIGNATION		NAME	SIGNATURE
Approved by	University President, De La Salle Araneta University	Dr. Bjorn S. Santos	 25 MAY 2017



## 5. Password Protection Policy

### Document Change Status:

Policy No./ Version No.	Date	Summary of Change
2017-4-Ver.1.0	March 2017	

Guidance: This policy should be read and carried out by all Administrators, Partners, Personnel, and Students who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DLSAU facility, has access to the DLSAU network, or stores any non-public DLSAU information.

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of IT resources. All users, including contractors and vendors with access to systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### 1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

### 2. Policies

#### 2.1. Password Creation

**2.1.1.** All user-level and system-level passwords must be eight (8) characters in length but not more than fourteen (14) characters and must contain an uppercase and lowercase text, a number and a special character.

**2.1.2.** Users must not use the same password for DLSAU accounts as for other non-DLSAU access (for example, personal ISP account, personal EMail, social media accounts, and so on).

**2.1.3.** Where possible, users must not use the same password for various access needs.

**2.1.4.** User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.

**2.1.5.** Users may not use their previous passwords when changing their password.

#### 2.2. Password Change

**2.2.1.** All system-level passwords (i.e. Active Directory, SERP, and so on) must be changed on at least on a quarterly basis. The recommended change interval is every three months.

**2.2.2.** All user-level passwords (i.e. email, web, desktop computer, and so on) must be changed at least every three months.



### **2.3. Password Protection**

- 2.3.1.** Passwords must not be shared with anyone. All passwords are to be treated as sensitive and confidential information.
- 2.3.2.** Final or active passwords must not be inserted into email messages or other forms of electronic communication.
- 2.3.3.** Passwords must not be revealed over the phone to anyone.
- 2.3.4.** Do not reveal a password on questionnaires or security forms.
- 2.3.5.** Do not hint at the format of a password (for example, "my family name").
- 2.3.6.** Do not share passwords with anyone, including administrative assistants, student assistants, secretaries, managers, co-workers while on vacation, and family members.
- 2.3.7.** Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- 2.3.8.** Do not use the "Remember Password" feature of applications (for example, web browsers).
- 2.3.9.** Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

### **2.4. Password Reset Changes**

Resetting system-level forgotten passwords must go to ICT Helpdesk service requests at **<http://itc-helpdesk/portal>** using Spiceworks App. The default or temporary password will be emailed on the official DLSAU Email Account and must be changed immediately for security by the user.

## **3. Administration**

The DLSAU ITC is the office-in-charge on the administration of this policy and the implementation of processes and procedures to ensure that the needed technical assistance is followed.

## **4. Applicability**

This policy applies to all passwords or any form of access that supports or requires a password in any system that resides at any DLSAU facility that has access to the DLSAU network.



## 5. Compliance

### 5.1. Compliance Measurement

The DLSAU ITC will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2. Exemptions


Any exception to the policy must be approved by the President/Chancellor in advance.

### 5.3. Non-Compliance

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**NOTE: This policy can be amended/modified/withdrawn at any point in time without any notice, at the discretion of the IT Council, duly authorized by the ITC Head and approved by the President/Chancellor, De La Salle Araneta University.**

**This policy will be effective in its entirety from March 2017 and will supersede all previous circulars/communication in this regard.**

DESIGNATION		NAME	SIGNATURE
Approved by	University President, De La Salle Araneta University	Dr. Bjorn S. Santos	 19 May 2017



## 6. Internet Usage Policy

### Document Change Status:

Policy No./ Version No.	Date	Summary of Change
2017-5-Ver.1.0	March 2017	

Guidance: This policy should be read and carried out by all Administrators, Partners, Personnel, and Students.

Internet connectivity exposes the institution with new risks that must be addressed to safeguard its IT facilities and vital information assets. These risks include misuse of IT resources and information. Excessive use of the internet may also adversely affect productivity due to time spent using or "surfing". All information found on the Internet should be not accurate until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Access to the Internet will be provided to users to support business activities and only on an as needed basis to perform their jobs and professional roles.

### 1. Purpose

The purpose of this policy is to define the appropriate usage of the internet by the DLSAU community.

### 2. Policies

#### 2.1. Internet Resource Usage

Allowed Internet Access and Usage will be during office/school hours only from 06:00 AM to 09:30 PM only from Monday to Sunday.

DLSAU Hotel and dormitories have 24 hours Internet Access and Usage but subjected to DLSAU's Firewall Policies.

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on the personnel's current job responsibilities. If personnel move to another business unit or changes job functions, a new Internet access request must be submitted. User Internet access requirements will be reviewed periodically by DLSAU ITC to ensure that continuing needs exist.



All Internet data that is composed, transmitted and/or received by DLSAU computer systems is considered to belong to DLSAU and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

Equipment, services, and technology used to access the internet are also property of DLSAU and has the right to monitor internet traffic and access data that is composed, sent and received through its online connections.

## 2.2. Allowed Usage

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

### 2.2.1. E-mail

Send/receive E-mail messages to/from the Internet (with or without document attachments).

### 2.2.2. Navigation

WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated DLSAU public web servers only.

### 2.2.3. File Transfer Protocol (FTP)

Send data/files and receive in-bound data/files, as necessary for business purposes only.

### 2.2.4. Telnet

Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the institution.

### 2.2.5. Research

Internet access is provided to users to support business activities and research only as needed to perform their jobs.

*Management reserves the right to add or delete services as business needs change or conditions warrant. **All other services will be considered unauthorized access to/from the Internet and will not be allowed.***

## 2.3. Personal Usage

Using the institution's computer resources to access the Internet for personal purposes that may hinder to perform their jobs and professional roles, without approval from the user's immediate head and the DLSAU ITC, may be considered cause for disciplinary action up to and including termination.



All users of the Internet should be aware that DLSAU network creates an **audit log** reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so **at their own risk**. DLSAU is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

#### 2.4. Prohibited Usage

Acquisition, storage, and dissemination of illegal or unauthorized electronic file or information that may expose the institution to liability and have an adverse impact on the institution's business, pornographic, or which negatively depicts race, sex or creed is specifically prohibited. DLSAU also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of students or personnel account information, unauthorized access of student or personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering student or personnel information. This includes making unauthorized changes to a student or personnel file or sharing electronic student or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the institution.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, national or international law including without limitations government export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all



materials on the Internet are copyright and/or patented unless specific notices state otherwise.

- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.
- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the DLSAU ITC and the user's immediate head.
- Any online ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.
- Installation of software apps such as instant messaging technology.
- Use of proxy sites, tunnelling sites or apps, and or VPN sites used for downloading or accessing blocked sites like PSiphon, Tunnelo, etc.
- Introducing malicious software unto the institution's network and/or jeopardizing the security of the network and manipulating the Technical Settings and Configurations of the network without written consent from the DLSAU ITC.

Bandwidth both within DLSAU and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other personnel. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.



**2.5. Request for Internet Access**

A written request is needed for special requests to access the internet and other special sites like social media sites addressed to the University President/Chancellor thru DLSAU ITC.

As part of the Internet access request process, all personnel are required to read both this Internet Usage Policy and the associated Internet/Intranet Security Policy as published thru DLSAU Institutional Bulletin (IB). Users not complying with these policies could be subject to disciplinary action up to and including termination.

**2.6. Approval**

Internet Access Requests will be approved by the University President/Chancellor thru DLSAU ITC.

**2.7. Removal of Privileges**

Internet access will be discontinued upon termination of personnel, completion of contract, end of service of non-personnel, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and a new request for access is approved. All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be re-evaluated by DLSAU ITC annually. In response to feedback from Administrators, Systems Administrators must promptly revoke all privileges no longer needed by users.

**2.8. Software License**

DLSAU strongly supports strict adherence to software vendors' license agreements. When at work, or when computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to DLSAU ITC for review or to request a ruling from the Legal Department before any copying is done. Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

**2.9. E-mail Confidentiality**

Users should be aware that clear text E-mail is not a confidential means of communication. DLSAU cannot guarantee that electronic communications will be private. The community should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

**2.10. Company Materials**

Users must not place DLSAU material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the user's immediate head and the Institutional Communications Office and will be placed by an authorized individual.

**2.11. Creating Web Sites**

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained from the University President/Chancellor thru DLSAU ITC. This will maintain publishing and content standards needed to ensure consistency and appropriateness. In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Institutional Communications Office for initial approval to continue. All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the DLSAU ITC.

**2.12. Usage Compliance Reviews**

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

**2.13. Policy Maintenance Reviews**

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit DLSAU information needs.



### 3. Administration

The DLSAU ITC is the office-in-charge on the administration of this policy and the implementation of processes and procedures to ensure that the needed technical assistance is followed.

Users should consider their Internet activities as periodically monitored and limit their activities accordingly. The Administration reserves the right to examine E-mail, personal file directories, web access, and other information stored on DLSAU computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the institution's information systems.

### 4. Compliance

#### 4.1. Compliance Measurement

The DLSAU ITC will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

#### 4.2. Exemptions

Any exception to the policy must be approved by the President/Chancellor in advance.


#### 4.3. Non-Compliance

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

In addition, DLSAU may at its discretion seek legal remedies for damages incurred as a result of any violation. DLSAU may also be required by law to report certain illegal activities to the proper enforcement agencies. Before access to the Internet via DLSAU network is approved, the potential Internet user is required to read this Internet usage Policy. For questions on the Internet Usage Policy, contact the DLSAU ITC.

**NOTE: This policy can be amended/modified/withdrawn at any point in time without any notice, at the discretion of the IT Council, duly authorized by the ITC Head and approved by the President/Chancellor, De La Salle Araneta University.**

**This policy will be effective in its entirety from March 2017 and will supersede all previous circulars/communication in this regard.**

	DESIGNATION	NAME	SIGNATURE
Approved by	University President, De La Salle Araneta University	Dr. Bjorn S. Santos	 19 MAY 2017





# Annex A. ICT Policy, Process & Procedures Manual Approval

The undersigned acknowledges that the said **ICT Policy, Process & Procedure Manual** was reviewed and agrees with the information presented within this document. Any changes to this document will be coordinated with, and approved by, the undersigned, or a designated representative.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print Name: \_\_\_\_\_

DR. BJORN S. SANTOS

Title: \_\_\_\_\_

PRESIDENT



Information Technology Center  
Rm 206B Life & Science Building  
De La Salle Araneta University

[www.dlsau.edu.ph](http://www.dlsau.edu.ph)