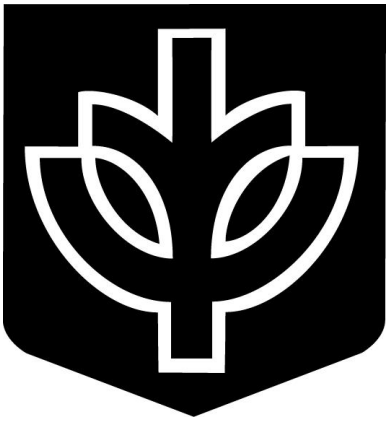
# ACCEPTABLE USE POLICIES
# FOR
# INFORMATION SERVICES COMPUTING RESOURCES



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604 US
https://infosec.depaul.edu/

13th December 2002

# Copyright Notice

# Contents

# 1 Summary

The DePaul University Information Services (IS) division provides an array of technology resources, ranging from Electronic Mail, Web hosting, internetworking connectivity and enterprise resource planning (ERP) business solutions, for use by the University, business peers and anonymous entities including Internet users.

This memo is intended to encourage, rather than discourage, the use of these, and other, IS resources by providing guidelines for acceptable use. All use of an IS resource shall constitute an implicit consent of the policies written herein. Violations of these acceptable use guidelines constitute a violation of IS policy requiring proper investigation by University personnel and state or federal law enforcement, where required.

# 2 Violations of Acceptable Use

The following actions, *incidental, accidental or purposeful,* are violations of this memo.

## 2.1 Illegal Use

Using any IS resource to transmit material or data (by email, upload, posting, etc.) that, intentionally or unintentionally, violates any applicable local, state, national, or international law, or express written rules defined per the IS department, violates acceptable use policies found in this memo.

## 2.2 Harmful Actions Towards Minors

Emloying any IS resource to harm, or attempt harm, to any minor or group of minors, or the collection of personal information of a minor, is a violation of this memo. A minor is any person under the age of eighteen (18) years of age.

## 2.3 Threats or Harassment

Transmitting material or data (by email, upload, posting, etc.) that encourages physical or intellectual damage, destruction of property, or harassment shall be considered a violation of this terms set forth within this memo.

## 2.4 Forgery or Impersonation

Falsifying or removing identifying information, in an attempt to deceive or misguide, is prohibited. Impersonation of any other person(s) in this manner constitutes violation of this policy. USENET postings in which email address header information has been altered to prevent targeting of data harvesters is allowed. Nicknames for online chat forums, messaging clients, Web site logins outside of the IS domain, etc. do not violate the terms of this memo.

## 2.5 Fraudulent Activity

Facilitating an IS resource to transmit any material or data (by email, upload, posting, etc.) that promotes a financial scam or wrong doing violate this memo.

## 2.6 Unsolicited Electronic Mail

Transmitting any material in the form of unsolicited electronic mail, unconfirmed email address subscription to mailing lists, or the subscription of email addresses to mailing lists without the ability to un-subscribe, is a violation of the terms within this memo.

## 2.7 Unauthorized Access, Threat Assessments, Penetration Tests

Threat assessments, penetration tests and other attempts to audit the integrity of IS resources, or remote network resources outside of IS, by means of port scanning, war dialing, and other hostile means, or unauthorized access to any user accounts, is a direct violation of this memo regardless of the success or harm committed to any resource(s) or data within those resource(s).

## 2.8 Intercepting Communications

The use of packet sniffers, password capture programs, keystroke loggers and other tools that perform promiscuous behavior on any systems maintained by IS, for any reason other than to monitor the data and network traffic authorized to an individual violates this memo.

## 2.9 Copyright or Trademark Infringement

Using any IS resource to transmit any material or data (by email, upload, posting, etc.) that infringes any copyright, patent, trademark, trade secret, or other proprietary right of an entity, whether online or not, violates the terms of this memo.

## 2.10 Collection of Personal Data

The collection of personal data as a means to harvest, analyze, profile or resell this data, without prior express consent from the target audience, violates this memo.

## 2.11 Reselling Services

Reselling services, including dial-up, electronic mail, Web hosting, file storage or processing time, without express written consent of the IS division violates this memo. Additionally, no service(s) provided by IS should be shared, leased, lent or resold at any time.

## 2.12 Network Interruptions

Using any IS resource to allow or promote any activity which adversely affects the ability of to access IS resources, or any other resource, both IS controlled or otherwise, violates this memo. Denial of Service attacks, spoofed packet transmission, and similar actions against, or originating from, any IS resource with malicious, or accidental intent, to cause delay or interruptions in services. In lieu of academic freedom, this violation does not pertain to academic research of such actions in controlled test environments authorized by the University.

## 2.13 Physical Security

Unauthorized access to, destruction or alteration of, theft, damage or tampering of any physical IS resource (including network cabling, wireless access points, computer workstations, kiosks, card readers, printers, audio-visual equipment, telephone equipment, FAX machine, computer room equipment or wiring closets) is a violation of the terms of this memo.

# 3 Reporting Violations of this Memo

## 3.1 Security Contact

The DePaul University Information Services department requests that any violations of this memo be reported immediately to the DePaul University Information Security Team (INFOSEC) for further investigation.

DePaul University Information Security Team <security@depaul.edu >

The use of digital signatures and strong encryption is *strongly* advised when reporting suspect activity; contact the response team for more information regarding this procedure, or visit the INFOSEC Web site at <https://infosec.depaul.edu >

## 3.2 Requested Report Information

The following information should be included when reporting any misuse of an IS computing resource —

1. The date and time, including Universal Coordinated Time (UTC offset), during which the alleged activity occurred.
2. Detailed descriptions of the activity.

Where possible, the following information should also be provided to assist in investigations —

1. The IP address used to commit any alleged activity.
2. Evidence of alleged activity.
3. Log information regarding the specific attack.
4. Packet traces of suspect network activity.
5. In the event of unsolicited email, an “inline”, forwarded, message, including all headers, should be included. Attachments will be discarded.

# 4 Response Handling

All reports submitted regarding computer or network abuse will be kept *confidential* by INFOSEC during investigation of the incident. INFOSEC shall advise University officials only in the event that a specific reaction, or increased escalation, is required.