

# Acceptable Use of Information Technology Resources

Effective: November 8, 2012  
Reviewed and Updated: February 17, 2020  
Contact: Information Technology Services (ITS)

## Contents

### Introduction

#### 1. Purpose

#### 2. Scope

#### 3. Policy Statement

#### 4. Unacceptable Use

##### 4.1. Excessive Non-Priority Use of Computing Resources

##### 4.2. Unacceptable System and Network Activities

##### 4.3. Unauthorized Use of Intellectual Property

##### 4.4. Inappropriate or Malicious Use of IT Systems

##### 4.5. Misuse of Electronic Communications

#### 5. Enforcement

##### 5.1. Interim Measures

##### 5.2. Suspension of Services and Other Action

##### 5.3. Disciplinary Action

### **Resources**

## Introduction

Iowa State University's Acceptable Use of Information Technology Resources policy (AUP) provides for access to information technology (IT) resources and communications networks within a culture of openness, trust, and integrity. In addition, Iowa State University is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

## 1. Purpose

The purpose of this policy is to outline the ethical and acceptable use of information systems at Iowa State University. These rules are in place to protect students, faculty, and staff; i.e., to ensure that members of the Iowa State University community have access to reliable, robust IT resources that are safe from unauthorized or malicious use.

Insecure practices and malicious acts expose Iowa State University and individual students, faculty, and staff to risks including virus attacks, compromise of network systems and services, and loss of data or confidential information. Security breaches could result in legal action for individuals or the university. In addition, security breaches damage the university's reputation and could result in loss of services. Other misuses, such as excessive use by an individual, can substantially diminish resources available for other users.

## 2. Scope

The AUP is an integral part of IT security policies and applies to faculty, staff, and students as well as any other individuals or entities who use information and IT resources at Iowa State University. This policy applies to all IT resources owned or leased by Iowa State University and to any privately owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, storage media, the campus network, and the Internet.

Securing and protecting these significant and costly resources from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the Iowa State University

47 community who accesses and uses IT resources. Therefore, every user of Iowa State University's IT  
48 resources is required to know the policies and to conduct their activities within the scope of the AUP,  
49 the Iowa State University **Information Technology Security policy**, and the **Policies, Standards,**  
50 **and Guidelines for IT Security** (see Resources below). Failure to comply with this policy may result  
51 in loss of computing privileges and/or disciplinary action.

### 52 **3. Policy Statement**

53 Unless otherwise specified in this policy or other university policies, use of university information  
54 technology resources is restricted to purposes related to the university's mission. Eligible individuals  
55 are provided access in order to support their studies, instruction, duties as employees, official  
56 business with the university, and other university-sanctioned activities. Individuals may not share  
57 with or transfer to others their university accounts including network IDs, passwords, or other access  
58 codes that allow them to gain access to university information technology resources.

59 Colleges, departments, and other administrative units have considerable latitude in developing  
60 complementary technology use policies and procedures, as long as they are consistent with this  
61 policy and any other applicable technology use policies of the university.

62 Incidental personal use of information technology resources must adhere to all applicable university  
63 policies. Refer to **Personal Use and Misuse of University Property policy** (see Resources below).  
64 Under no circumstances may incidental personal use involve violations of the law, interfere with the  
65 fulfillment of an employee's university responsibilities, or adversely impact or conflict with activities  
66 supporting the mission of the university.

### 67 **4. Unacceptable Use**

68 Users are prohibited from engaging in any activity that is illegal under local, state, federal, or  
69 international law or in violation of university policy. The categories and lists below are by no means  
70 exhaustive, but attempt to provide a framework for activities that fall into the category of  
71 unacceptable use.

#### 72 **4.1. Excessive Non-Priority Use of Computing Resources**

73 Priority for the use of IT resources is given to activities related to the university's missions of  
74 teaching, learning, research, and outreach. University computer and network resources are limited in  
75 capacity and are in high demand. To conserve IT resource capacity for all users, individuals should  
76 exercise restraint when utilizing computing and network resources. Individual users may be required  
77 to halt or curtail non-priority use of IT resources, such as recreational activities and non-academic,  
78 non-business services.

#### 79 **4.2. Unacceptable System and Network Activities**

80 Unacceptable system and network activities include:

81 **4.2.1.** Engaging in or effecting security breaches or malicious use of network communication  
82 including, but not limited to:

83 **4.2.1.1.** Obtaining configuration information about a network or system for which the user  
84 does not have administrative responsibility.

85 **4.2.1.2.** Engaging in activities intended to hide the user's identity, to purposefully increase  
86 network traffic, or other activities that purposefully endanger or create nuisance traffic for the  
87 network or systems attached to the network.

88 **4.2.1.3.** Circumventing user authentication or accessing data, accounts, or systems that the  
89 user is not expressly authorized to access.

90           **4.2.1.4.** Interfering with or denying service to another user on the campus network or using  
91 university facilities or networks to interfere with or deny service to persons outside the  
92 university.

### 93 **4.3. Unauthorized Use of Intellectual Property**

94 Users may not use university facilities or networks to violate the ethical and legal rights of any  
95 person or company protected by copyright, trade secret, patent, or other intellectual property, or  
96 similar laws or regulations. Violations include, but are not limited to:

97 **4.3.1.** Except as provided by fair use principles, engaging in unauthorized copying, distribution,  
98 display, or publication of copyrighted material including, but not limited to, digitization and distribution  
99 of photographs from magazines, books, or other copyrighted sources; copyrighted music or video;  
100 and the installation of any copyrighted software without an appropriate license.

101 **4.3.2.** Using, displaying, or publishing licensed trademarks, including Iowa State University's  
102 trademarks, without license or authorization or using them in a manner inconsistent with the terms of  
103 authorization.

104 **4.3.3.** Exporting software, technical information, encryption software, or technology in violation of  
105 international or regional export control laws.

106 **4.3.4.** Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.

107 **4.3.5.** Using computing facilities and networks to engage in academic dishonesty prohibited by  
108 university policy (such as unauthorized sharing of academic work or plagiarism).

### 109 **4.4. Inappropriate or Malicious Use of IT Systems**

110 Inappropriate or malicious use of IT systems includes:

111 **4.4.1.** Setting up file sharing in which protected intellectual property is illegally shared.

112 **4.4.2.** Intentionally introducing malicious programs into the network or server (e.g., viruses, worms,  
113 Trojan horses, email bombs, etc.).

114 **4.4.3.** Inappropriate use or sharing of university-authorized IT privileges or resources.

115 **4.4.4.** Changing another user's password, access, or authorizations.

116 **4.4.5.** Using an Iowa State University computing asset to actively engage in displaying, procuring, or  
117 transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws,  
118 or other illegal activity.

119 **4.4.6.** Using an Iowa State University computing asset for any private purpose or for personal gain.

### 120 **4.5. Misuse of Electronic Communications**

121 Electronic communications are essential in carrying out the activities of the university and to  
122 individual communication among faculty, staff, students, and their correspondents. Individuals  
123 should also read and follow the university's **Mass Email and Effective Electronic**  
124 **Communication Guide** (see Resources below).

125 Prohibited misuses of university electronic communications include:

126 **4.5.1.** Sending unsolicited messages, including "junk mail" or other advertising material, to  
127 individuals who did not specifically request such material, except as approved under the Mass  
128 Email and Effective Electronic Communication Guide.

129 **4.5.2.** Engaging in unlawful harassment as defined by State and Federal law.

130 **4.5.3.** Masquerading as someone else by using their email or internet address or electronic  
131 signature.

132 **4.5.4.** Soliciting email from any other email address, other than that of the poster's account, with  
133 the intent to harass or to collect replies.

134 **4.5.5.** Creating or forwarding "chain letters" or solicitations for business schemes.

135 **4.5.6.** Using email originating from Iowa State University provided accounts for commercial use or  
136 personal gain.

137 **4.5.7.** Iowa Code section 68A.505 and Iowa Administrative Code Chapter 351-5 prohibit public  
138 bodies and public employees from using public resources for political purposes, including expressly  
139 advocating the nomination, election, or defeat of a candidate and/or expressly advocating the  
140 passage or defeat of a ballot issue. For additional information and examples of prohibited use of  
141 public resources, see Iowa Administrative Code Chapter 351-5.

## 142 **5. Enforcement**

143 The Acceptable Use of Information Technology Resources policy is enforced through the following  
144 mechanisms.

### 145 **5.1. Interim Measures**

146 The university may temporarily disable service to an individual or a computing device, when an  
147 apparent misuse of university computing facilities or networks has occurred, and the misuse:

148 **5.1.1.** Is a claim under the Digital Millennium Copyright Act (DMCA)

149 **5.1.2.** Is a violation of criminal law

150 **5.1.3.** Has the potential to cause significant damage to or interference with university facilities or  
151 services

152 **5.1.4.** May cause significant damage to another person

153 **5.1.5.** May result in liability to the university

154 An attempt will be made to contact the person responsible for the account or equipment prior to  
155 disabling service unless law enforcement authorities forbid it or Information Technology Services  
156 staff determine that immediate action is necessary to preserve the integrity of the university network.  
157 In any case, the user shall be informed as soon as possible so that they may present reasons in  
158 writing why their use is not a violation or that they have authorization for the use.

### 159 **5.2. Suspension of Services and Other Action**

160 Users may be issued warnings, may be required to agree to conditions of continued service, or may  
161 have their privileges suspended or denied if:

162 **5.2.1.** After hearing the user's explanation of the alleged violation, an IT provider has made a  
163 determination that the user has engaged in a violation of this code, or

164 **5.2.2.** A student or employee disciplinary body has determined that the user has engaged in a  
165 violation of the code.

### 166 **5.3. Disciplinary Action**

167 Violations of the Iowa State University Acceptable Use of Information Technology Resources policy  
168 may be referred for disciplinary action as outlined in the Student Disciplinary Regulations and  
169 applicable faculty and staff handbooks or collective bargaining agreement. The university may  
170 assess a charge to offset the cost of the incident.  
171

## 172 **Resources**

### 173 **Links**

- 174 • [Information Technology Security policy](#)
- 175 • [Electronic Privacy policy](#)
- 176 • [Personal Use and Misuse of University Property policy](#)
- 177 • [Mass Email and Effective Electronic Communication policy](#)
- 178 • [Student Disciplinary Regulations \(Code of Conduct\)](#)
- 179 • [Acceptable Use of Information Technology Resources \[Policy in PDF with line numbers\]](#)
- 180 • [Social Media Guidelines \[PDF\]](#)

181