

# **Sample Responsible Use of Computing Policy**

## **I. Scope**

This policy applies to all persons who use the Company's Computing Resources, including but not limited to Company employees, clients, visitors, and contractors.

## **II. Policy Statement**

The Company provides and maintains its general computing services to support the work of its employees. At the same time, the Company desires to protect all users' rights to an open exchange of ideas and information.

This policy sets forth the responsibilities of the users of the Company's Computing Resources.

Because it is impossible to anticipate all the ways in which individuals can damage, interrupt, or misuse the Company's Computing Resources, this policy focuses on a few simple rules.

This policy allows for investigations of complaints involving the misuse of the Company's Computing Resources, including complaints of sexual harassment, violations of the Company's Honor Code, and violations of federal, state, and local laws. Violations of this policy may result in revocation of access, suspension of accounts, disciplinary action including dismissal, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities.

## **III. Definitions**

The "Company's Computing Resources" means all computers, systems, workstations, networks, networking equipment, peripheral devices, servers, and any other Company property attached to the Company's network. The Company's Computing Resources also include all software, programs, files, documents, and databases stored in the Company's computing systems.

"Information Technology Services (ITS)" means the Company department that is responsible for IT equipment and services within the Company's system.

"User" means any person who uses the Company's Computing Resources.

## **IV. Compliance**

Access to the Company's Computing Resources is a privilege granted on a presumption that every member of the Company's community will responsibly exercise this privilege by preserving the security, confidentiality, availability, and integrity of the Company's Computing Resources.

It is the responsibility of all Users to read and follow this policy and all applicable laws and procedures. In addition, when using the Company's Computing Resources, Users must adhere to the following rules:

**RULE 1: Use the Company's Computing Resources only for the purpose of supporting the needs of the Company.**

- Users may not use the Company's Computing Resources for recreation or entertainment if such use interferes with the needs of the Company.

**RULE 2: Do not use the Company's Computing Resources to violate other policies or laws.**

- Do not use the Company's Computing Resources to violate laws or Company policies, including but not limited to the Company's Honor Code, Human Resources policies, or Standards of Conduct.
- Do not extend the Company's network without explicit permission from ITS Network Engineering and Technology. The unauthorized use of routers, switches, wireless access points, and other devices is prohibited by Company policy.
- Do not use the Company's Computing Resources to transmit, store, display, download, print, or intentionally receive obscene material.

**RULE 3: Use only the Company's account(s) you are authorized to use.**

**RULE 4: Do not use any of the Company's Computing Resources for inappropriate purposes.**

A non-exhaustive list of example restrictions follows:

- Do not sell access to the Company's Computing Resources.
- Do not engage in commercial activity not sanctioned by the Company, except for incidental personal use.
- Do not intentionally deny or interfere with any network resources.
- Do not use or access any of the Company's Computing Resources, or read or modify Company-owned files, without proper authorization.
- Do not use the Company's Computing Resources to in any way misrepresent or impersonate someone else.
- Do not violate copyright laws and licenses.
- Do not violate Company policy or federal, state, or local laws.

**RULE 5: Honor the privacy of other Users.**

- Do not access the contents of another User's files without express authorization from that User.

- Do not intercept or monitor any network communications meant for another person or purpose.
- Do not transmit or distribute personal or private information about individuals without express authorization from the individuals affected.
- Do not create or use programs, *e.g.*, keyloggers that secretly collect information about Users.

**RULE 6: Do not allow another User to access your accounts.**

Users may be held responsible for actions related to their specific account(s). If a person violates any policies, his or her actions can be traced back to the username, and the account holder may be held responsible.

**V. Company Responsibilities**

The Company acknowledges that personal email, electronic files, and websites maintained on Company equipment are part of an electronic information environment. While this policy endeavors to maintain User confidentiality, it cannot create, nor should Users presume, any expectation of privacy.

The Company reserves the right to inspect all User files and communications for all lawful purposes, including but not limited to investigating allegations of illegal activity, violations of Company's policies, or to protect the integrity and security of network systems. The Company will investigate all complaints involving personal web sites hosted on Company resources and will remove or block material or links to material that violate federal or state law or Company policy.

The Company considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information on Company Computing Resources related to suspected unacceptable use and to protect its resources from systems and events that threaten or degrade operations.

The Company may choose to suspend a User's access to its resources in connection with an investigation. Users are not entitled to any expectation of privacy. User files, network transmissions, computer sessions, data, and/or communications may be shared with appropriate investigating officials.

**VI. Sanctions**

The consequences of policy violation will be commensurate with the severity and frequency of the offense and may include termination of employment.

In addition, consequences of policy violation may include, but are not necessarily limited to, the following:

- Notification—alerting a User to what appears to be an inadvertent violation of this policy in order to educate the User to avoid subsequent violations.

- Warning—alerting a User to the violation, with the understanding that any additional violation will result in a greater penalty.
- Loss of computer and/or network privileges—limitation or removal of computer and/or network privileges, either permanently or for a specified period of time.
- Restitution for damages—requiring reimbursement for the costs of repair or replacement of computer-related material, equipment, hardware, software, data and/or facilities; such reimbursement shall include, but not necessarily be limited to, the cost of additional time spent by Company employees due to the violation.
- Penalties—if applicable, the violator may be subject to criminal or civil penalties.

The violation of copyright, licenses, or personal privacy or the publishing of obscene materials or child pornography may result in civil or criminal legal actions as well as Company disciplinary actions.

## **VII. Copyright Infringement**

Because the Company is the Internet Service Provider (ISP) for the Company community, it is held to strict copyright compliance standards and other mandates. The process described here, called “No More,” will be used to communicate with Users alleged to have violated copyright law. This process will be employed when Company’s Computing Resources have been used to download or upload media illegally using peer-to-peer file sharing software or other methods.

The Company does not actively search for instances of copyright infringement or monitor a specific individual’s network activity. However, notices of copyright violations affiliated with an individual’s account are cumulative throughout his/her time at the Company.

### No More - #1 Notice

1. The User is made aware that illegal infringing activity may have taken place via his/her Company account.
2. The User is required to remove the stated infringing material and any peer-to-peer file sharing software used for this purpose from his/her computer.

### No More - #2 Notice

1. The User is made aware that this is the second instance of illegal infringing activity on his/her Company account. Receipt of a second notice generally indicates a pattern of downloading rather than a single, incidental event.
2. The User is required to remove the stated infringing material and any peer-to-peer file sharing software used for this purpose from his/her computer.

3. The User must meet with Company leadership, within a prescribed time, to discuss alternative, legal sources of in-copyright content.
4. The User must write, sign and date a letter stating that the infringing materials and peer-to-peer file sharing software have been removed from his/her computer. The Company retains this letter.
5. If the User does not meet with the Company leadership within the prescribed time, that individual will be partitioned from the Company network until such time the Stop It #2 requirements are fulfilled.

#### **VIII. Dates**

A. Effective Date: The policies herein are effective \_\_\_\_\_. This policy shall be reviewed and revised, if necessary, annually.

B. Date of Most Recent Review: \_\_\_\_\_, 2018

#### **IX. Timetable for Review**

This policy, and any related procedures, shall be reviewed annually or more frequently as needed.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

**RESPONSIBLE USE OF COMPUTING POLICY**

**ACKNOWLEDGMENT**

**Employee Name:** \_\_\_\_\_

**Employee Position:** \_\_\_\_\_

**Date of Receipt of Responsible Use of Computing Policy:**

I acknowledge and agree that:

- (1) I have received a copy of the Company Responsible Use of Computing Policy;
- (2) I have read the Responsible Use of Computing Policy in its entirety and fully understand the provisions contained therein; and
- (3) I agree to abide by the provisions contained in the Responsible Use of Computing Policy.

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Employee's Name (Printed)

\_\_\_\_\_  
Date