SECURITY AWARENESS AND ACCEPTABLE USE POLICY

Overview

Southern Research is committed to protect all employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity, but are needed to assure this protection.

All systems, including but not limited to computer equipment, hardware, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and file transfer, are the property of Southern Research. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving participation and support from every Southern Research employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Southern Research. These rules are in place to protect the employees and Southern Research. Inappropriate use exposes Southern Research to risks including malicious software, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at Southern Research, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Southern Research.

Policy

General Use and Ownership

1. While network administration desires to provide a reasonable and corporate level of privacy, users should be aware that the data they create on the corporate systems remains the property of Southern Research.

2. Any information that users consider sensitive or vulnerable must be encrypted.

3. For security and network maintenance purposes, authorized individuals within Southern Research may monitor equipment, systems and network traffic at any time.

4. Southern Research reserves the right to audit networks and systems including individual use on a periodic basis to ensure compliance with this policy.
Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorized access to confidential and/or sensitive information. The information contained on all systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, research data and any data classified by customers as confidential.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords must be changed every 90 days.

3. All desktops, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.

4. Employees should secure their workstations by logging off or locking the screen (control-alt-delete for Windows users) when unattended.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Information Technology will enable hard drive encryption on all portable computers.

6. All computer equipment used by the employee that is connected to Southern Research networks, must be property of Southern Research.

7. All computer equipment must be continually executing approved virus-scanning software with a current virus database.

8. Employees should not open any e-mail attachments received from unknown senders, which may contain malicious software.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Southern Research authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Southern Research owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Southern Research.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Southern Research does not have an active license is strictly prohibited.

3. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all Southern Research properties is prohibited unless required as part of a job function or as outlined in other Southern Research policies, or authorized by a corporate officer.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Export Control specialist should be consulted prior to export of any material that is in question.

5. Introduction, installation and/or play of any type of games and/or video gaming entertainment software to any computer device including desktops, laptops and servers as well as the use of local or Internet network bandwidth for this purpose.

6. Introduction, installation, viewing and/or listening of non-work related videos, movies, music, e-books, etc. to any computer device including desktops, laptops and servers as well as the use of local or Internet network bandwidth for entertainment purposes.

7. Use, introduction and/or installation of any Internet File Sharing hosting service to temporary or permanently store and/or transmit Southern Research’s information (e.g. Drop Box, Amazon Cloud Drive, Amazon S3, Google Drive, Apple iCloud, MS One Drive, etc.).

8. Introduction and/or installation of malicious programs into any computer systems and network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

9. Revealing your account password to others or allowing use of your account by others. This includes coworkers, family and other household members when work is being done at home.

10. Allowing non-employees access to your assigned personal computer or any Southern Research equipment unless the non-employee has a written labor agreement with Southern Research for consulting or other specific work and has signed a non-disclosure agreement. Non-employees include family and other household members when devices are brought home.

11. Using a Southern Research computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

12. Making fraudulent offers of products, items, or services originating from any Southern Research account.

13. Making statements about warranty, expressly or implied, unless it is a part of normal job duties and is consistent with Southern Research’s Standard Terms and Conditions in effect at the time such statement is made or approved by the General Counsel.
14. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

15. Port scanning or security scanning is expressly prohibited unless prior notification to Information Security is made.

16. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

17. Circumventing user authentication or security of any host, network or account.

18. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

19. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

20. Providing information about, or lists of, Southern Research employees to parties outside Southern Research.

21. Use of certain web and social media sites (e.g. Facebook, Twitter, etc.) are blocked, but if an employee has a legitimate business purposes, please notify the Director or VP in your group in writing to allow for access.

Corporate Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material, to individuals who did not specifically request such material (email spam) is prohibited unless per a management approved marketing program.

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7. Posting by employees from Southern Research’s email address to newsgroups or Social Media sites without the proper authorization of the General Counsel and Government Affair’s offices.

8. Employees must not utilize Public Instant Messaging software (e.g. Yahoo, MSN, etc.).
9. Employees must not utilize third-party e-mail systems to communicate and/or transfer Southern Research’s information, files, contacts, etc. (e.g. Hotmail, Gmail, Yahoo, AOL, etc.)

10. Employees will not refer to clients/sponsors by name or by their products on personal social networks in any fashion, nor divulge or hint at any confidential information learned as part of their employment with Southern Research. This applies to posting on Social Media sites (e.g. Facebook, Instagram, Twitter, etc.) personal or professional blogs, newsletters or blog comments.

**Enforcement**

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

**Definitions**

*Spam* Unauthorized and/or unsolicited electronic mass mailings.

---

Employee/Contractor/Third Party Signature

Date

Printed Name