Electronic Communications and Communication Systems Policy

OBJECTIVE

Use of the information systems and computer networks of Cirrus Logic, Inc. and its affiliated companies (the “Company”) is critical to the Company’s success. The Company invests substantial resources to provide and maintain systems essential to our business operations. Employees are responsible for adhering to the highest standards in all of their computer usage and communications. This Electronic Communications and Communication Systems Policy (the “Policy”) is intended to ensure Company’s electronic resources are used in a manner that:

- Serves the purpose intended (i.e., to support our businesses);
- Supports other Company policies;
- Sustains employee productivity;
- Maintains the Company’s good reputation;
- Protects the confidentiality of Company and third-party information; and
- Limits the possibility of damage to and unauthorized access and use of Company systems and data.

SCOPE

This Policy applies to all of the Company’s communications systems and computer networks and every Company employee, as well as external consultants, temporary staff, and third party contractors. Its terms are subject to any applicable local legal and/or regulatory requirements.

During the course of your engagement with the Company, the Company may provide you access to various systems, including, but not limited to the Company’s network, computers, workstations, software, hardware, Internet/Intranet/Extranet, electronic messaging systems (for example email and instant messaging), fax machines, voice mail, phones, and tablets.

POLICY STATEMENT

Right to Access/Privacy

All computer and telecommunications systems and all communications and information transmitted by, received from, or stored in these systems are under the control of the Company and are intended for business use. Please understand that you should have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt or storage of information with this equipment including the use of personal equipment connected to Company networks and communication systems. Employees may wish to consider using alternative methods to send and receive private messages. To the extent authorized by applicable laws, the Company may monitor and/or record electronic communications such as the retrieval of particular email messages or the monitoring of internet usage. The purpose of such activities is generally to protect the Company against employee misconduct and to ensure that the communication systems are being used consistent with applicable Company policies, but may also be to enable us to locate Company messages or data, to comply with our legal obligations, or for other business purposes. Your consent to such monitoring and recording is presumed by your use of the Company’s communication systems.

While the Company does not actively monitor, record, and review its employees’ electronic and telephonic communications, it has the technical capability of doing so and reserves the right to do so. This may include, among
Electronic Communications and Communication Systems Policy

other things, monitoring the use of Company computers and personal devices accessing Company networks and communication systems. In all cases in which electronic monitoring and/or recording is carried out, it will be conducted in accordance with all applicable laws and regulations, and any active monitoring and/or recording will be authorized by the Company’s General Counsel.

Appropriate Uses

All forms of electronic communications should be treated the same as any other formal business communications and should be conducted in a professional, responsible, and courteous manner. Although electronic communications facilitate quick and convenient communications with others, written electronic communications can be particularly troublesome since they may often be misunderstood or misinterpreted due to their frequent casual nature. Since some types of electronic communications can be easily forwarded, they can inadvertently or intentionally be sent to unintended recipients. Therefore, employees should bear in mind that their electronic communications may be read and heard by someone other than the person to whom they are sent and may be disclosed to outside parties or a court in connection with litigation or government investigations.

You may not send, display, or store any material, in any format, that violates any Company Policy. Content must not:

- Be harassing, offensive, obscene, derogatory, or disparaging based on, for example, an individual’s sex, race, color, religion, age, national origin, marital status, ancestry, sexual orientation, veteran status, disability, medical condition, pregnancy, or citizenship status;
- Reflect any illegal activity or create the possibility of negatively affecting the Company's reputation;
- Be used for personal financial benefit or support non-Company commercial purposes;
- Be pornographic, offensive, threatening, or defamatory; or
- Violate any trademark, copyright, or software licensing contract, rule, or regulation.

Violations of this Policy may result in disciplinary action, up to and including termination of employment.

Personal Use

Limited personal use of the Company’s Communication Systems is permitted so long as it does not interfere with job performance, consume significant resources and time, give rise to more than nominal additional costs, or interfere with the activities of the employee’s job responsibilities and duties. However, even with respect to limited personal use, you should have no expectation of privacy in connection with the use of Company equipment or systems.

Employees should note that the Company utilizes third party service providers in connection with its system security and its back-up processes. Data on the Company’s hardware, including employee laptops, may therefore be accessible by third parties, and other Company staff, in connection with such processes. Any access to such data shall be in accordance with applicable laws. However, employees are encouraged to refrain from including personal or private information on their drives, and particularly file folders subject to third-party backup services (for example, home and user folders), and to consult with IT regarding any questions about backed-up folders or related settings.

Except as specifically authorized by the Company, participation in chat rooms, on-line forums, blogs, bulletin and message boards, social media or non-Company instant messaging may be considered communications with the public and should not take place in connection with Company business or through Company systems. For example, you may not post messages regarding any confidential, non-public information about Cirrus Logic or any other company that you learn about as a result of your employment with Cirrus Logic.
Electronic Communications and Communication Systems Policy

If you do participate in posting messages that do not involve Cirrus Logic or the confidential information of other companies, any postings made must be for personal use only and should not be used to reflect Company policy or opinions. You are responsible for your activities on social media, blogs, and message boards, and you assume all liability for your actions.

Confidential Information/Security

The Company has an obligation to maintain the confidentiality of its own information and information of third parties that may be communicated through the Company’s electronic communications system. As a consequence, all users of the Company’s electronic communications system must take steps to ensure the security of the system and to maintain the confidentiality of all email and other information on the system or communicated through the use of the Company’s electronic communications system.

Although we require passwords to access most Company electronic communication systems, the use of passwords for security does not guarantee confidentiality. When you are provided a username and/or password, you are responsible for both keeping the password confidential and for all activity conducted under that username and password. You are also accountable for information entered into or maintained on the computer assigned to you.

Please notify a Systems Administrator promptly if you have any reason to believe your username and/or password have been compromised.

Cloud Services

While cloud storage services offer many benefits, the Company cannot control their security measures or guarantee that they will adequately protect our confidentiality. Therefore, you should not store any confidential Company or third-party information on a non-Company communication system. For example, do not use services such as iCloud, Evernote, Dropbox, Google Drive, Box, Sky Drive, Amazon Cloud Drive, etc. to store or transfer confidential Company or third-party documents or information. If you need to transfer confidential Company or third-party information that is too large to send by email, please use the Company’s secure file-transfer protocol. Please ask the IT Department if you need help using this service.

If you use a cloud storage service with respect to non-confidential information, any such use must comply with all other Company policies. If you are unsure whether a certain document or piece of information is confidential, you should err on the side of concluding it is confidential or ask the Legal Department for help.

Exceptions to this section of the policy require the approval of the IT and Legal Departments.

Downloads/Software/Outside Files and Disks

Software and files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet; files from newsgroups, bulletin boards, or other online services; files attached to emails; and files provided by customers or vendors, may contain dangerous computer viruses, which may damage Company’s electronic information resources. When using software and files obtained from sources outside the Company, employees should use good judgment, and should consider scanning those files with Company-approved virus checking software prior to use. If you suspect that a virus has been introduced into the Company’s network, please notify a System Administrator immediately.
Electronic Communications and Communication Systems Policy

Retention and Litigation

Electronic communications users are accountable for understanding and complying with corporate and departmental document retention requirements. Electronic communications are to be handled in the same manner as written communications. If you have any questions about document retention guidelines, please see the Company's Document Retention Policy or contact the Legal Department.

Electronic communications are forms of recorded communication and may be subject to pre-trial discovery, used as evidence during legal proceedings, or used in response to regulatory inquiries involving the Company, its subsidiaries, agents, or individual employees. Courts and regulatory bodies may impose sanctions if the Company fails to adequately preserve and protect the content and integrity of electronic communications that are responsive to a discovery request, including, but not limited to, voicemail, text messages, instant messages, email, Word documents, Excel spreadsheets, and PowerPoint presentations. Once you have knowledge of a legal or regulatory inquiry, or believe that such an inquiry is imminent, you must preserve and protect all electronic communications or other documents relating to that matter. If you have any questions about which electronic communications should be retained, contact the Legal Department.

Violations

Users who violate any provisions of this Policy may be subject to disciplinary action, up to and including termination.

QUESTIONS

For more information or clarification of any of the provisions in this Policy, please contact your System Administrator or a representative of the Legal Department.