INFORMATION SYSTEMS ACCEPTABLE USE POLICY

This Policy is designed to protect Logitech, our employees, customers and other partners from harm that could result from misuse of our electronic systems, devices or network resources. The stakes are high as our information systems provide the backbone of our operations and any misuse can result in significant issues such as confidential information leaks, data breaches, identity theft, degraded operations, lost productivity and civil or criminal penalties.

Each of us is responsible for exercising care and good judgment while using Logitech's information systems and in keeping them secure. Logitech is committed to protecting you, our partners and customers and the company from illegal and damaging actions by others as much as reasonably possible.

ACCESS

You are given **access** to Logitech information systems to **perform your job**. Your access should never be used for any unlawful or prohibited purpose including:

- Making unlicensed copies of copyrighted songs, movies, pictures etc.
- Sending spam or misusing group emails
- Harassing or threatening another individual
- Posting or sharing confidential information without authorization
- Speaking on behalf of Logitech without authorization
- Concealing or misrepresenting your identity or the source of a message
- Violating any Logitech policy

You also **may access** Logitech information systems **for reasonable personal** use as long as it does not interfere with your job performance or otherwise negatively impact the company. Please always be thoughtful and responsible in your business and personal use of our systems.

Any user leaving the company must relinquish all access to Logitech's information systems and return all company devices and data.

Please see Logitech's **Privacy, Sexual Harassment and Confidential Information** policies and our Social Media guidelines for further guidance. If you are uncertain about the appropriateness of any online activity or other usage of our information systems, please ask Logitech Legal or email us at **compliance@logitech.com**

SECURITY

You are responsible for the security of data, accounts, and systems that you use. You should always follow IT's guidelines for creating and changing passwords and keeping them secure. You should not share account or password information with anyone, including family or friends. Providing access to another unauthorized individual, either deliberately or through failure to secure its access, violates this Policy. Likewise, you should not forward Logitech e-mail or any other data to personal accounts.

Please **be vigilant in maintaining the security of your devices** as any one of our devices can become a gateway for a data breach, cyber attack or other harmful actions. Time-tested preventive measures are the best tools at our disposal for maintaining device security. Please always employ the following guidelines:

WHAT SHOULD I DO IF MY DEVICE IS LOST OR STOLEN?

Immediately contact the Global Security Operations Center (GSOC) at **lsecurity@logitech.com** and notify your mobile carrier.

DON'T BE CARELESS WITH YOUR DEVICES

- Store and transport your Logitech and personal devices securely
- Minimize the amount of confidential information on mobile devices
- Don't let others use your devices
- Don't share your device PIN or password

BE THOUGHTFUL ABOUT WHERE YOU PUT LOGITECH DATA

- Do not store or back up Logitech email or Logitech data on third party services (e.g., iCloud)
- Backup devices regularly
- If your device syncs to third party services (e.g., iCloud), use strong passwords, change them frequently and always ensure that you do not synch Logitech email or data

USE THE TOOLS WE PROVIDE

- Follow IT's PIN code and dual level-authentication guidance
- Use encryption as required by IT when transmitting or storing Logitech data
- Always install and keep up to date security software mandated by Logitech IT

PERSONAL DEVICE USAGE

Logitech allows you to "bring your own device" (BYOD) and use it with Logitech email and certain other Logitech applications and data. Our BYOD program is entirely voluntary. IT will validate the basic security settings of your personal devices and non-compliant devices will be denied access. IT may deactivate access or quarantine any personal device upon detection of a data breach, violation of law or policy, virus or other threat to security.

Please remember that by using your own device to access or store Logitech data you are agreeing to give Logitech access to the device as it may be necessary for the company to access and collect data for business or legal needs.

Also keep in mind that you are solely responsible for your personal device. **Logitech will not reimburse you for any lost, stolen or damaged personal devices**, and IT is not obligated to provide any hardware or software support for personal devices.

PRIVACY

Logitech respects and protects your right to privacy as required by governing law. Logitech will not collect, process, and/or store your personal information except where required for reasons directly linked to your employment.

Logitech uses system health, security and performance monitoring technologies. These activities are focused on the health of our information systems and devices, not your individual activities as a user. Logitech, however, employs remote maintenance, which means that **IT may access your device** and all its applications. This process will **only be used for maintenance purposes** and you will be informed by IT beforehand.

Logitech will only access your company email, IM and stored data if required to by law or if Logitech is investigating potential illegal activities or potential company policy violations. **Logitech DOES NOT review the content of emails or folders clearly marked as "Personal."** If you have personal items you want to keep private, please keep your personal data segregated from Logitech data and label it as such.

SCOPE AND CONSEQUENCES

This Policy applies to employees, contractors, consultants, temporary workers and anyone else given access to Logitech information systems or devices. If any local law conflicts with this Policy, the Policy will be interpreted as adjusted to comply with such law.

Violations of this Policy may result in disciplinary action including temporary or permanent removal of your access, reprimand or even termination of your employment or business relationship with Logitech. Logitech also reserves the right to initiate criminal or civil actions. Please note that you may have dispute resolution rights under local law depending on where you are located.

QUESTIONS?

If you have any questions or concerns about this Policy, please raise them with your manager or a representative from People & Culture, IT or Legal. Also, you can email **compliance@logitech.com** for guidance on this Policy.