CRESTRON ELECTRONICS, INC.
CRESTRON PRIVACY STATEMENT REGARDING INTERNET DATA COLLECTION

This Privacy Statement explains Crestron’s practices regarding the collection, use and disclosure of end-user information transmitted via the Internet from certain Crestron products. COLLECTED INFORMATION IS TRANSMITTED TO SERVERS AT CRESTRON FACILITIES AND/OR TO CLOUD-BASED STORAGE, CONTROLLED BY CRESTRON AND/OR THIRD PARTIES, WHICH MAY BE LOCATED IN THE UNITED STATES OF AMERICA (USA) AND OTHER COUNTRIES.

1. CERTAIN CRESTRON PRODUCTS TRANSMIT END-USER DATA

Crestron transmits and/or collects end-user data via the Internet, through the use of certain Crestron products, including: (a) Crestron Mobile Apps that are loaded onto end-user mobile devices, (b) Cloudware products, such as Crestron Fusion®, and (c) hardware Devices, such as Crestron® 3-Series® processors and TSW-x60 Touch Screens. The end-user data collected and/or transmitted by these Crestron products is detailed below.

2. END-USER CONSENT TO DATA TRANSFER

By using a Crestron Mobile App, Crestron Cloudware, or a Crestron Device, you consent to the transfer of your data as described in this Privacy Statement, which may be updated by Crestron from time to time, with the latest version available at https://www.crestron.com/legal-data-collection-privacy.

By using a Crestron Mobile App, you also consent to the Terms of Use for Crestron Mobile Apps, which may be updated by Crestron from time to time, with the latest version available at https://www.crestron.com/legal-mobile-apps-tou.

3. GENERAL PRIVACY POLICY

Crestron routinely collects certain information during our normal course of business. For example, Crestron may collect information when you visit our website, register a product, attend one of our events or request more information from us. Crestron’s collection and use of this information is detailed in Crestron’s general Privacy Policy, which may be updated by Crestron from time to time, with the latest version available at http://www.crestron.com/legal/privacy-policy.

4. CRESTRON DOES NOT ACCEPT SENSITIVE PERSONAL INFORMATION

Crestron refuses to accept and you agree not to provide Crestron with any access to sensitive personal information including in particular: (a) national identification numbers; (b) financial information; (c) information about children; (d) criminal records; (e) health information; (f) information regarding an individual’s physical, physiological, mental, economic, cultural, or social identity; and (g) biometric data.

5. CRESTRON AUTHORIZED INTEGRATORS MAY COLLECT ADDITIONAL DATA

Crestron controlled systems are programmed by third party Crestron Authorized Integrators and/or Crestron Service Providers, who may be retained directly by end-users, to provide a customized experience for end-users, and meet their individual needs. These Authorized Integrators may program end-users’ systems to collect or transmit data in a manner that is not listed in this Privacy Statement, based on the arrangements made directly between the end-user and their Authorized Integrator and/or Service Provider. Crestron does not limit the ability of Authorized Integrators and/or Service Providers to program Crestron controlled systems to transmit additional information over the Internet or to collect additional data.

6. DATA COLLECTION BY CRESTRON MOBILE APPS

Crestron Mobile Apps may be preloaded on devices distributed by or on behalf of Crestron, or may be downloaded and installed from a third-party application distribution channel such as, the Apple® iTunes® App Store®, Google Play™ Store, and the Microsoft® Windows® Phone Store. The type of information which may be collected by Crestron Mobile Apps is detailed below.

6.1 AirMedia® and Crestron Shading Solutions Mobile Apps do not collect information.

6.2 Crestron App, Crestron Mobile®, Crestron Mobile Pro®, Mobile G®, Mobile Pro G®, Crestron Beacon Setup Pro, Crestron Home Beacon Setup, Crestron Zūm™ and Crestron Pyng® Mobile Apps collect Mobile App registration information, which includes the IP address associated with your device. Crestron Pyng requires an end user to create a myCrestron account, described below.

6.3 Crestron PinPoint™ collects Mobile App registration information and may also transmit the location of Crestron Pinpoint Mobile App users within a building utilizing Crestron Pinpoint beacons, if those features are activated.
7. **DATA COLLECTION BY CRESTRON CLOUDWARE PRODUCTS**

CRESTRON CLOUDWARE PRODUCTS REQUIRE A CONTINUOUS CONNECTION TO THE INTERNET TO FUNCTION, AND WHEN CONNECTED TO THE INTERNET, CONTINUOUSLY UPLOAD AND DOWNLOAD INFORMATION FROM CONNECTED DEVICES TO CRESTRON’S CLOUD BASED STORAGE.

7.1 Crestron Cloud-Based Provisioning and Management Platform collects the following information: (a) Cloudware License information; (b) “Approximate Geographic Location”, based on postal code and/or latitude/longitude; (c) “Connected Device Information”, including IP addresses, SIP addresses, firmware versions, room names, device names, scene settings, configuration settings and associations between buttons and device functions; and (d) “Log Information” regarding usage of Crestron controlled equipment and devices.

7.2 Crestron Fusion and Crestron Scheduling Cloudware collects the following information: (a) Approximate Geographic Location; (b) Connected Device Information; (c) Log Information; (d) “Meeting Scheduling Information”, which may include, meeting date, time, subject, location, attendees, and invitees; and (e)”Business Contact Information” of attendees or invitees, which may include name, title, address, email contact and phone number.

8. **DATA COLLECTION BY CRESTRON HARDWARE DEVICES**

CERTAIN CRESTRON DEVICES, INCLUDING SOME CATEGORIES OF PROCESSORS AND TOUCH SCREENS, AUTOMATICALLY TRANSMIT INFORMATION WHEN INSTALLED AND CONNECTED TO THE INTERNET.

8.1 Crestron® 3-Series® Processors

Crestron 3-Series Processors that automatically attempt to establish Internet communication include, but may not be limited to: (a) PRO3, (b) AV3, (c) CP3 and CP3N, (d) DIN-AP3 and DIN-AP3MEX, (e) MC3 and RMC3, (f) FT-TSC600, (g) TPCS-4SM, and (h) PYNG-HUB.

Once connected to the Internet, via your Internet service provider, your Crestron 3-Series Processors will periodically upload information including: (a) Approximate Geographic Location; (b) Connected Device Information; (c) Configuration Data for the Crestron Processors, including connected devices, room names, device names, scene settings, and associations between buttons and device functions, in source code format; (c) Log Information; and (d) software diagnostic information.

8.2 Crestron® Mercury™ Tabletop Conference System

A Crestron Mercury™ Tabletop Conference System will automatically attempt to establish Internet communication with Crestron and other third party servers.

Once connected to the Internet, via your Internet service provider, the Crestron Mercury™ Tabletop Conference System will periodically upload the following: (a) Cloudware License Information; (b) Approximate Geographic Location; (c) Connected Device Information; (d) software diagnostic information; and (e) third party authentication information, as described below.

8.3 Crestron Touch Screens

Crestron Touch Screens that automatically attempt to establish Internet communication with Crestron and other third party servers include, but may not be limited to: (a) TSW-552, (b) TSW-752, (c) TSW-1052, (d) TSW-560, (e) TSW-760, and (f) TSW-1060.

Once connected to the Internet, via your Internet service provider, the Crestron TSW-x52 and TSW-x60 Touch Screens will periodically upload the following: (a) Approximate Geographic Location; (c) software diagnostic information; (d) third party authentication information. When voice recognition features on these devices are activated, recorded voice commands and translated text files are transmitted to Crestron and/or its third-party service providers, who may be subject to their own privacy policies, as detailed below.

9. **myCrestron ACCOUNT INFORMATION**

The use of certain Crestron products and services, including Crestron Pyng or remote monitoring services, may require you to create a myCrestron account. When you create a myCrestron account, Crestron will collect and store your email address and the URL associated with your Crestron System. From that point forward, your email address may be used for communications from Crestron regarding your associated Crestron products and services.

10. **DATA COLLECTED BY THIRD PARTY SERVICE PROVIDERS**

10.1 Third Party Add-On Content Provided by Crestron

Crestron may make available to its end-users certain third party add-on features or content that can provide an enhanced experience, including but not limited to, Internet weather, radio. Use of these features or content may provide end-user information, such as Approximate Geographic Location or IP address to these third party providers.
CRESTRON ELECTRONICS, INC.
CRESTRON PRIVACY STATEMENT REGARDING INTERNET DATA COLLECTION

10.2 Data Collected by Third Parties that Require a Separate End-User Account

Use of certain third party apps, for example, Amazon Alexa®, Skype® for Business, Sonos® Controller, or Zoom™, on a Crestron device, requires the end-user to have an active account with that third party. In order to allow the use of such third party apps by a Crestron device or service, Crestron collects and stores the end-user profile and/or account information which is required for third party authentication, and transmits that information to the third party. Such third party authentication information for a third party app typically includes, but may not be limited to: (a) user id, (b) user e-mail address, (c) password, and (d) SIP address.

Third party apps may also collect and use information about each end-user and their use of these apps, subject to their own privacy policies, and not under the control of Crestron.

10.3 Voice Recognition Features

Certain Crestron products include voice recognition features, provided in connection with third party service providers, such as for example, Amazon Alexa® and Google Voice™. For these products, recorded voice commands, consisting of speech detected after a ‘push-to-talk’ or detection of a key phrase, such as “O.K. Crestron”, is transmitted to servers at third party facilities and/or to cloud-based storage, each located in the United States of America (USA) and other countries.


In the case of Google Voice, voice data transmitted to Google is subject to “Google APIs Terms of Service” and the “Google Privacy Policy”, located at https://developers.google.com/terms/, and https://www.google.com/policies/privacy/.

11. HOW CRESTRON USES YOUR INFORMATION

Crestron will use the information collected by its end-user products and software development tools to: (a) provide services, (b) improve system functionality and performance, and (c) gather troubleshooting and configuration backup information. Crestron will also use this information to assess system efficiency and to offer improvements and personalized options in order to enhance the end-user experience, which may be used to provide certain system functionality, such as weather reporting, and local TV station listings.

Crestron employees, contractors and affiliates, including our service technicians, have supervised access to your information as required to provide services, troubleshoot your system and monitor our servers for technical problems.

Crestron may share your aggregated and anonymous information for a variety of purposes, including marketing and improvement of Crestron products and services. This aggregated and anonymous information cannot be linked back to you.

Except as described herein, we will only provide information collected by Crestron to a third party, other than your Authorized Integrator, if required to do so by law, or in the good-faith belief that such action is necessary to comply with state and federal laws or respond to a court order, subpoena, or search warrant.

12. HOW LONG CRESTRON WILL STORE YOUR INFORMATION

Crestron will store the information collected by (i) Crestron Mobile Apps, (ii) Crestron Devices, and (iii) Crestron Cloudware for as long as you remain a customer of the associated Crestron products and services. Because of the way Crestron maintains its server data, after your information is deleted, backup copies may linger for some time before they are deleted.

13. HOW CRESTRON PROTECTS YOUR INFORMATION

Crestron understands the importance of the safety and security of your information and takes precautions to protect your personal information against loss, theft, misuse and unauthorized access. For that reason, Crestron has implemented safeguards to protect your personal information in accordance with industry standards.

To protect any data stored on Crestron servers or cloud-based storage, we regularly monitor our systems for vulnerabilities or attacks.

Access to personally-identifying information that is stored by Crestron is limited only to those of its employees, contractors and affiliated organizations that need to know that information in order to process it on Crestron’s behalf and that have agreed not to disclose it to others.
CRESTRON ELECTRONICS, INC.
CRESTRON PRIVACY STATEMENT REGARDING INTERNET DATA COLLECTION

14. OPTING-OUT OF DATA COLLECTION

OPTING OUT OF DATA COLLECTION WILL PREVENT CLOUDWARE AND CERTAIN CRESTRON MOBILE APPS FROM FUNCTIONING, AND MAY LIMIT THE AVAILABLE FEATURES AND SUPPORT FOR OTHER CRESTRON DEVICES AND MOBILE APPS.

15. CONTACT CRESTRON

Crestron will address inquiries regarding personal information promptly and courteously. If you want to delete your personal information from Crestron’s servers, and/or Crestron’s cloud-based storage, opt out of data collection, or have other inquiries, please contact us at support@crestron.com.

TRADEMARK DISCLAIMER

Certain trademarks are used herein to refer to either the entities owning the marks or their products. Crestron disclaims any proprietary interest in the marks of others.