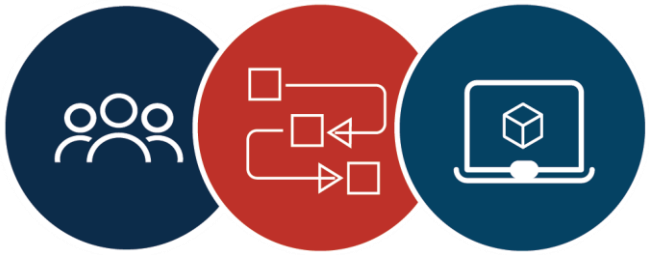
Important Product Safety & Service Information

Please read carefully
Before using any Convergint-installed solution

Convergint Technologies LLC and its affiliates ("Convergint") provide security, fire and life safety, audio-visual, building automation, and other services and solutions to its customers based on third party, commercially available products. It is imperative that users of any Convergint-provided services and solutions read the following safety information and warnings prior to using the solutions, as well as warnings and documentation provided by third party product manufacturers or developers.

EFFECTIVE SECURITY AND SAFETY IS A MULTI-LAYERED APPROACH INVOLVING PEOPLE, PROCESSES, AND TECHNOLOGIES.



CONVERGINT-PROVIDED SERVICES AND SOLUTIONS ARE ONLY ONE PARTY OF THIS MULTI-LAYERED APPROACH.

UNDER NO CIRCUMSTANCES SHOULD YOUR CONVERGINT-INSTALLED SOLUTION BE YOUR SOLE METHOD OF SECURITY OR SAFETY.

IMPORTANT NOTICES FOR ALL SOLUTIONS

Testing & Maintenance: Test the solutions on a regular basis, confirm the solutions are functioning properly, promptly address any malfunctions (including by seeking support from Convergint or the original product manufacturer as needed), and maintain the solutions in accordance with the original product manufacturers' usage instructions, terms, and conditions. Except as otherwise agreed in a service plan, testing and maintenance is **CUSTOMER'S RESPONSIBILITY** — and where Convergint has agreed to test or maintain the solutions on a periodic basis, it is still **CUSTOMER'S RESPONSIBILITY** to test and maintain during interim periods.

Training: Implement appropriate hiring, retention, and training processes for users of the solutions, to ensure that all users have received adequate training, and to ensure the solutions are used in a manner consistent with product manufacturer usage instructions, terms, and conditions. Convergint may have training programs available for your solutions — ask your Convergint point of contact for more information.

Software: Perform all necessary software updates and maintenance for software that is part of or will be used in conjunction with the solutions. **FUNCTIONALITY OF THE SOLUTIONS AND YOUR NETWORK'S INFORMATION SECURITY MAY BE COMPROMISED IF YOUR SOFTWARE IS NOT UP-TO-DATE.** Except as otherwise agreed in a service plan, software updates and maintenance is **CUSTOMER'S RESPONSIBILITY**. Convergint may have password and software patch management programs available for your solutions — ask your

Convergint point of contact for more information.

Information Systems and Networks: Restrict access to the solutions to trusted and authorized users and implement best practices for access management, including password management, multi-factor authentication, monitoring usage, and proper information security and confidentiality training. Ensure networks on which the solutions are installed are properly secured in accordance with information security best practices. To the extent Convergint is granted access to Customer's information systems, Convergint agrees to follow or use Customer-specified policies or methods. However, **CUSTOMER IS ULTIMATELY RESPONSIBLE FOR THE INFORMATION SECURITY OF ITS INFORMATION SYSTEMS AND DATA**, including any third party products connected to its networks and overall system security.

Service Plans: If you have a service plan, you must provide accurate information to Convergint, update Convergint with any changes that may be relevant to the solutions, and provide Convergint with reasonable access to Customer systems and facilities. **FUNCTIONALITY MAY BE IMPAIRED IF THE INFORMATION PROVIDED TO CONVERGINT IS INACCURATE OR OUTDATED, OR ADEQUATE ACCESS IS NOT PROVIDED.**

Original Manufacturer Claims: Convergint does not independently validate the accuracy of marketing claims or product capability representations made by original product manufacturers. **YOUR RELIANCE ON THESE CLAIMS IS AT YOUR OWN RISK**.

IMPORTANT NOTICES REGARDING ALARMS & NOTIFICATIONS

Certain solutions, including mass notification systems, are intended to assist in the detection of emergencies or events that may threaten lives, bodily injury, or property. In the event of an emergency, **YOU MUST TAKE NECESSARY ACTION TO PREVENT SERIOUS PROPERTY DAMAGE, INJURY, OR DEATH FROM OCCURRING.** These actions include, but are not limited to, the following:

- Calling 9-1-1;
- Executing your emergency action and/or evacuation plan;
- Accounting for all individuals in or on the premises;
- Providing medical assistance as needed;
- Contacting the necessary security, safety, or emergency personnel;
- Ensure all applicable personnel are trained in the proper operation of alarm and notification systems; and
- Ensure you have a back-up notification system in place

IMPORTANT NOTICES FOR THREAT DETECTION SOLUTIONS

Certain solutions are intended to detect specific threats, such as weapons detection, gunshot or shooter detection, and drone detection systems. These systems can help detect, but will not eliminate, risks of loss associated with the threats, and may not detect all types of threats. System sensitivity settings can materially impact the extent to which these solutions detect threats, including which threats are detectable. These systems are not intended to be a replacement for a multi-layered and vigilant approach to security. These Convergint-provided systems **MUST ALWAYS BE USED IN CONJUNCTION WITH ADDITIONAL SAFETY MEASURES**.

convergint

IMPORTANT NOTICES FOR HEALTH EMERGENCY DETECTION

Certain solutions are intended to monitor for and detect health emergencies. These systems do not, and are not intended to provide, medical advice or treatment. These solutions should only be used under the guidance of licensed medical professionals, whose advice should always be followed. These solutions **SHOULD NOT BE RELIED UPON AS THE SOLE MEANS OF DETECTING A HEALTH EMERGENCY**. If you are responsible for caring for individuals at risk of a medical emergency, you must take the necessary precautionary and planning measures, which may include consultation with and following advice of a licensed medical professional; routine wellness checks; developing and communicating an action plan in the event of a medical emergency; calling 911 in the event of a medical emergency; providing necessary life-saving measures, to the extent you are qualified to do so; and informing the necessary individuals in the event of a medical emergency.

IMPORTANT NOTICES FOR BIOMETRICS

Certain solutions are intended to authenticate or assist in the recognition of individuals using biometric technologies (such as, for example, facial recognition, retina or iris scanning, and fingerprint or hand geometry scanning). Biometric technologies are regulated in many jurisdictions, and you may be required to (among other requirements) provide notice to, and receive consent from, individuals whose biometric data is being processed. **CONSULT WITH A LICENSED ATTORNEY FOR THE APPROPRIATE JURISDICTION BEFORE ENABLING ANY BIOMETRIC CAPABILITIES**. **CUSTOMER IS SOLELY RESPONSIBLE FOR COMPLYING WITH BIOMETRIC REGULATIONS.**

IMPORTANT NOTICES FOR ARTIFICIAL INTELLIGENCE

Certain solutions are intended to identify security or safety related threats using artificial intelligence. Artificial intelligence technologies are new, have a limited track record, and are not fail-proof. Such systems should always be used as part of a multi-layer program that includes additional technologies as well as additional human- and process-based checks and balances. Artificial intelligence systems may also have the potential of inadvertently introducing bias into security programs — you should proactively monitor for and take steps to remediate any such bias.

⚠WARNING!	
	**Always call 911 in the event of an emergency.**

convergint

⚠ WARNING!	
	Convergint systems typically require power and a network connection to function properly. **YOUR CONVERGINT SYSTEM MAY NOT WORK IN THE EVENT OF A POWER OUTAGE OR WIRELESS NETWORK OUTAGE.** Rely on a multi-layered approach to security and plan for possible power or wireless network outages.