VIRALERT
SAFE | EASY | ACCURATE

LAND
AMETEK

GUIDELINES FOR COMPLIANCE WITH DATA PROTECTION WHEN INSTALLING A **TEMPERATURE SCREENING SYSTEM**

As the economy starts to reopen, businesses are responding quickly to changes in everyday activities in order to resume operations. Moreover, health authorities across the globe are guiding and updating on key procedures and requirements for businesses to safely bring employees, customers and visitors back on site.

One important tool in this effort is temperature screening for all who enter a business, retail store or any public location. Temperature screening identifies potentially symptomatic people and prevents them from exposing others. Fixed, non-contact temperature screening systems utilizing thermal imaging technology, like the VIRALERT (www.landviralert.com), are simple to use and reliable solutions.

Systems like the VIRALERT are not intended to detect medical conditions such as viruses or other illnesses. An elevated temperature should be confirmed with a secondary evaluation method, such as an approved medical thermometer. Skin temperature varies depending on several factors, including environmental conditions, and does not always reflect body temperature.

Unlike handheld thermometers which compromise social distancing rules, non-contact, thermal imaging screening systems can be easily installed and provide accurate, contactless skin temperature measurement of personnel at the point of entry. As the measurement is taken in seconds, screening can be achieved with minimal impact on the flow of people.

It is important to note that temperature screening solutions like VIRALERT may have the ability to capture and store information in addition to temperature – such as faces, which may be considered protected as personal data under various country, state, region and local laws.

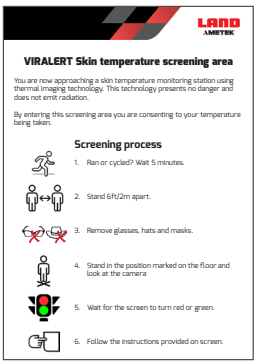
While human body temperature alone is often not defined as private, data protection laws vary globally and may apply, particularly if a person can be identified using the information captured. For this reason, it is important for users to have policies and/or processes in place to address the capture, storage, transmission and availability of any private data generated.

The VIRALERT has been designed with these data privacy considerations in mind, and includes user-selected configurations where no data is stored to increase privacy and reduce compliance risk. However, if users choose to store potential personal data, in addition to seeking legal advice steps should be taken to ensure compliance with data privacy rules.

AS YOU EVALUATE OPTIONS FOR A TEMPERATURE SCREENING SOLUTION, THE FOLLOWING GUIDELINES IDENTIFY SOME OF THE MAJOR CONSIDERATIONS TO KEEP IN MIND:

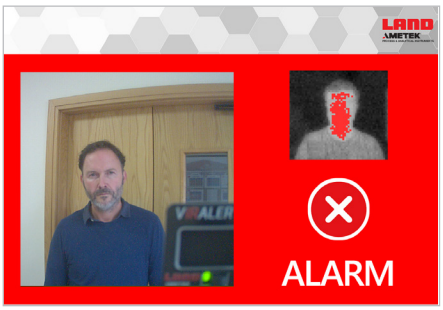
CONSENT

Individuals should know that their temperature is going to be taken and should understand the ramifications if they choose not to participate in the screening. For this reason, it is advisable to establish a written policy and to post notices regarding the use of temperature screening. Screening station posters are available for download from the VIRALERT website. In addition, you may want to consider a signed consent for the screening of visitors.



ELEVATED TEMPERATURE

An elevated temperature based on initial screening should be confirmed with a secondary evaluation method, such as an approved medical thermometer. It is not advisable to take action against an individual based on a skin temperature check unless it is confirmed by a clinical-grade device.



STORED DATA

Temperature screening solutions like VIRALERT may have the ability to capture and store information in addition to temperature. As a general guideline, any data that you collect should be no more than is needed, and should be appropriately controlled. When possible and as part of good data practices, the need should be documented along with its rationale.

Data should also only be kept for a reasonable period of time, and a policy to delete data after this time is recommended. The VIRALERT system has a feature to automatically delete user data after a configurable time-period, making this maintenance task simple and easy.

STORAGE LOCATION

The data produced by the VIRALERT system is, by default, saved onto the local computer's hard drive. In this case, the local hard drive should be encrypted, and the computer password-protected. Further measures, such as physical protection of the computer from theft and using software to disable USB drives, should also be considered to ensure data is protected.

The VIRALERT system can also be configured to store data on user-selectable network locations. If data is not stored on the local hard drive, care should be taken to ensure that access to the selected file location is limited to people for whom the data is relevant.

LAND AMETEK®

CONTACT US

landviralert.com

land.enquiry@ametek.com

Certificate No. CC-2041
Applies in India

Applies in the UK

Applies in the US

