Wi-Fi Security Statement

All Viessmann internet-connected HVAC-systems ('Heating, Ventilation & Air-Conditioning'-systems) maintain the highest standards for security and follow industry best practices:

- All information exchanged between Viessmann HVAC-systems, Viessmann servers & Viessmann Apps is encrypted.
- Viessmann uses industry-standard protocols to secure each HVAC-system's Wi-Fi connection.

1) Local direct connection to the HVAC-system:

- A local direct connection to the HVAC-system allows the installer or a Viessmann service technician to e.g. commission the homeowner's system via the ViStart app. When connecting locally to the system, WPA2 is used to secure the connection. For a local direct connection to the HVAC-system, an internet connection is not required (instead the HVAC-system opens a 'Wi-Fi access point' to which the installer or the Viessmann service technician can then connect to).
- When opening a local direct connection, it is required to enter the WPA2-key on the device that is used to locally connect to the HVAC-system (e.g. smartphone, tablet or notebook). The WPA2-key can be found on the sticker that is attached to the side of the HVAC-system and/or in the service manual. It is not possible to locally access the HVAC-system without the WPA2-key. Data will only be transferred from the used device to the connected HVAC-system.

2) Remote connection to the HVAC-system via homeowner's Wi-Fi network:

- To be able to remotely access the HVAC-system, it is required to connect the HVAC-system to the homeowner's Wi-Fi network and enter the network password (if not already done so, Viessmann strongly recommends that the network password is encrypted via WPA2).
- A remote connection via the homeowner's Wi-Fi network allows the homeowner to remotely control the HVAC-system e.g. via the ViCare app. It also allows an installer or Viessmann to remotely monitor and access the homeowner's system, for example to provide better remote support via Vitoguide in case of a system malfunction (note: the

homeowner's consent, a so-called "opt-in", is required for the installer or Viessmann to be able to remotely access the homeowner's system. The homeowner can give his consent electronically via ViCare).

- No information about the homeowner's Wi-Fi network (e.g. SSID or passwords) is transmitted to Viessmann servers.

Further information:

- When accessing the HVAC-system locally (via its 'Wi-Fi access point') or when accessing the device remotely via the customer's Wi-Fi network, it is not possible to access any other devices that are connected to the customer's Wi-Fi network.
- Viessmann does not use port forwarding or require any router ports to be opened.
- In cases where the homeowner's Wi-Fi network credentials have changed, for example when switching to a new internet service provider, then the homeowner needs to re-connect the HVAC system using the new Wi-Fi network credentials. Viessmann has no access to the homeowner's Wi-Fi network credentials and cannot perform this task.
- If a homeowner sells his/her home together with their Viessmann HVAC-system, then the previous homeowner should de-register the HVAC system installation in ViCare. The new homeowner can then link the HVAC-system installation with his/her own ViCare-account. (note: should the previous homeowner forget to de-register the installation and cannot be contacted, then it is recommended that the new homeowner contacts the Viessmann support).

To help maintain a secure HVAC-system, Viessmann:

- Continuous security upgrades of all controller firmware and software
- Employs both internal and external system auditing
- Consults with independent security companies to ensure we are following best practices
- Performs full code penetration testing