SMART HOME CYBER SECURITY MANIFESTO

The manifesto comprises the following recommendations for the industry across three categories, data security, data policy and consumer support:

DATA SECURITY

1. The smart home must be secure by design – Security cannot be added as an afterthought. Products and services must be secure across design, development, promotion and maintenance stages, and throughout the entire supply chain.
2. The smart home must be able to authenticate all users – From knowing your heating preferences, to recommending which movie to watch, it is vital that everyone connected to the home network can be accounted for.
3. All data that flows through the smart home must be encrypted – This is especially true of the personal and financial data of users.
4. More must be done to ensure end-to-end security – As most smart home devices and services will connect through the cloud and other data centres, each step must be secure and not endanger the end-user.

DATA POLICY

5. Companies must adopt transparent data policies – It must be made explicitly clear what personal data is collected and what that data is then used for. Consumers must be told if any company sells their data to marketers or any other third-party.
6. All smart homes must offer the same level of privacy as homes do now. That means when the doors are closed, and the curtains pulled down, no company or person should expect to be able to access any activity of the home owner.

CONSUMER SUPPORT

7. All smart home devices and services must be accessible and understandable for all users, regardless of technical prowess – The end-user should never be blamed for a security vulnerability that arises in the installation or the running of a product or service.
8. All devices and services must launch with lifetime support – This means regular security updates and on-going support for the consumer for as long as the product or service is live.

The Smart Home Security Manifesto was written by CONTEXT with input gratefully acknowledged from Dixons Carphone, SH&BA, Intel, D-Link, Mathembedded, Qonex, Deutsche Telekom, Euronics, and Nottingham University.

CONTEXT