



THE SECURED BY DESIGN 10-POINT SECURITY GUIDE FOR

Heat Pumps, Battery Storage Systems & EV Charging Cables

Heat pumps, battery storage systems and electric vehicle (EV) charging cables are now common in new and refurbished homes. They are key to the UK's net zero transition, supporting energy efficiency, low-carbon living, and smart home integration. With the Future Homes Standard removing gas from all new developments and upgrades required across an estimated 26 million homes, these technologies will become standard in communities nationwide.

But their value also makes them a target. Thieves and vandals damage or remove copper pipework, cabling, batteries, control systems and other valuable components. Entire installations have been stolen or destroyed, causing expensive repairs, disruption and reduced public confidence.

This guide sets out Secured by Design's (SBD) layered approach to reducing these risks. It provides practical, evidence-based crime prevention measures to deter, delay, detect and enable response to criminal activity.

As the official police security initiative, SBD works with manufacturers, designers, installers and academia to embed effective security from the outset. By applying proven standards, these assets can be secured without compromising efficiency, accessibility, or integration, supporting safe, resilient, and sustainable homes.

This guidance was produced with support from the Building Alliance and the Centre for Future Homes at Birmingham City University.



1 Siting and Positioning

- 1.1 Whilst units should be sited as close to the building as possible to minimise pipe runs, reduce heat loss and maintain airflow/service clearances, avoid installations where the unit, brackets or nearby features facilitate climbing to ledges, overhangs, low roofs, balconies or upper floors.



Detached or Semi-Detached Homes with Rear Gardens or Side Access

- 1.2 The most secure position is a private rear garden, protected by a locked gate and boundary fencing at least 1.8m in height.
- 1.3 Where only side access is available, this can also be secure if sited behind a 1.8m (minimum height) locked gate and compliant fencing, supplemented by other protective measures described in this guide.

Detached or Semi-Detached Homes without Rear Gardens or Side Access

- 1.4 If a front installation is the only option, place the unit as close to the building as possible to minimise pipe runs, reduce heat loss and maintain airflow/service clearances, in clear view - not hidden behind walls, hedges, bins, or parked vehicles - and overlooked by active rooms (see *Note 1.4*) and, ideally, neighbouring homes. This maximises natural surveillance by enabling neighbours and passers-by to notice, challenge, or report suspicious activity. Avoid installations where the unit, brackets or nearby features facilitate climbing to ledges, overhangs, low roofs, balconies or upper floors.

Note 1.4: An 'active room' is a living space with regular occupancy and outward visibility, such as a kitchen, dining room, or lounge. Bedrooms and bathrooms are not considered active rooms.

Flats and Apartments

- 1.5 Units serving flats and apartments without private gardens, should ideally be installed in secure, restricted-access service areas such as locked plant rooms or roof spaces, while maintaining maintenance access.
- 1.6 If ground-floor flats require units to be installed at the front of the building, see Section 1.4.



2 Perimeter Security

- 2.1 Side and rear gardens should be enclosed with boundary fencing at least 1.8m in height. Trellis and defensive planting can provide extra height and protection.
- 2.2 Side gates should be the same height as the fence, set as close to the front building line as possible, fitted with SBD compliant locks, and secured with protected or non-removable hinges.



3 Physical Protection of Units

- 3.1 Fix units to a concrete base with tamper-resistant bolts or ground anchors that can't be easily removed with standard tools.
- 3.2 Where the risk is higher, use galvanised steel security cages with anti-tamper fixings. Cages must allow airflow, servicing, and be compatible with manufacturer specifications. This will also help prevent deliberate or accidental damage and reduce the risk of fingers entering fan areas.
- 3.3 Run cabling internally where possible. For external runs, use steel conduit or armoured cable.
- 3.4 Reinforce cable entry points with tamper-resistant clamps and fittings.



4 Property Marking

- 4.1 Mark external units with the property's postcode or address using chemical etching or permanent UV marking. Check that this doesn't affect the warranty.
- 4.2 Apply forensic property marking liquid (e.g. SmartWater, SelectaDNA) to key components and register them on a secure ISO27001-compliant database (or equivalent). This links recovered items to the rightful owner and assists police investigations.
- 4.3 Display signage to highlight forensic marking, which can often be as effective as the marking itself in deterring theft.



5 Tracking and Monitoring

- 5.1 Consider discreet GPS trackers or transponders inside the unit casing, with tamper alerts, backup power, and real-time location tracking.
- 5.2 Register devices with a monitoring service or integrate them with the home security system.



6 Lighting and Surveillance

- 6.1 Install dusk-to-dawn lighting to illuminate the unit and its surroundings.
- 6.2 If using a video surveillance system (VSS), securely mount cameras with a clear view of the unit. Ensure compliance with GDPR when monitoring public areas. Further advice is available from the Information Commissioner's Office: <https://ico.org.uk>
- 6.3 Footage should be clear and of high quality, night-capable, and securely stored. Display signs to indicate surveillance monitoring.
- 6.4 Position cameras to avoid obstructions such as planting, direct sunlight, or shadows that reduce effectiveness.
- 6.5 Fit tamper alarms to units where possible, integrated with the main intruder alarm system. These should activate if the unit is lifted, its casing removed, or its power interrupted.



7 Installation Timing and Site Management

- 7.1 Don't install units until the site is secured with fencing, gates and access controls.
- 7.2 If units are delivered early, they must be stored securely. In domestic settings, all security products - including locks, bolts, video surveillance, alarms and padlocks - should be SBD-accredited. Installers should ensure units are kept in a locked garage or container with lighting, and ideally VSS and/or an intruder alarm. Padlocks must be high quality and protected by lock boxes (cowlings). If secure storage is not available, delivery should be delayed until the day of installation.
- 7.3 Building sites are especially vulnerable, particularly when unoccupied, and require robust protection. Secure metal containers should be used, with all security products SBD accredited. Measures should include lighting, video surveillance, intruder alarms and clear signage. Containers must not be placed on the perimeter where they can be attacked from outside the site, and padlocks must be high quality and shielded by lock boxes. Storage units should be covered by detector-activated VSS. For high-value equipment, tagging systems (e.g. SmartWater or SelectaDNA) that spray intruders with a forensic solution can be used, leaving a unique trace that increases the likelihood of identification, arrest and prosecution. Regular checks or patrols should also be carried out on unoccupied sites.

Further guidance on police preferred security products is available at:
<https://www.securedbydesign.com>
- 7.4 Ideally, install external units at the final stage of build/renovation to minimise theft and damage risks.



8 Battery Storage Units

- 8.1 Install battery storage systems in secure locations, with lockable, weather-resistant enclosures, securely fixed to a concrete base using tamper-resistant bolts or ground anchors. Avoid locating batteries within dwellings due to fire and escape risks. Apply similar precautions to e-bike and e-scooter storage and refer to the National Fire Chiefs' Council guidance for battery fire-safety information: <https://nfcc.org.uk/our-services/campaigns/e-bikes-and-e-scooters-fire-safety-guidance>.
- 8.2 Place units within gated boundaries (see Section 2) or areas with strong natural surveillance, and where feasible, protect with video surveillance and dusk-to-dawn lighting.



9 Smart Connected Heat Pumps

- 9.1 The Product Security and Telecommunications Infrastructure Act 2022 requires minimum security for connected consumer devices, based on ETSI EN 303 645.

- 9.2 Change default credentials and keep firmware/software up to date to mitigate cyber security threats.
- 9.3 Use encrypted communication protocols, secure networks, and multi-factor authentication where possible to protect remote access.
- 9.4 SBD's Secure Connected Device accreditation scheme, developed with the Department for Science, Innovation and Technology, assesses Internet of Things (IoT) devices against ETSI provisions and enables certified products to display the SBD accreditation mark. Further information is available at: <https://www.securedbydesign.com/internet-of-things/secure-connected-devices>



10 Electric Vehicle (EV) Charging Cables

- 10.1 EV charging cables are high-risk theft targets due to the value of the internal copper wiring. Disconnect and store them securely when not in use, particularly overnight.
- 10.2 Install EV charge points with tamper-resistant fixings. Protect cable routes with steel conduit or through-wall connections. Position units in visible, well-lit areas close to the property, overlooked by active rooms (see *Note 1.4*), neighbours, and passers-by to maximise natural surveillance.

Conclusion

Heat pumps, battery storage systems, smart connected devices, and EV charging cables are high-value, vulnerable assets. This risk increases during the installation phase due to the value of the parts rather than resale, but this may change as the market size increases.

By following SBD's layered approach - siting, visibility, physical protection, property marking, surveillance and robust cyber security – developers and homeowners can significantly reduce risks, protect investment and support public trust in sustainable technologies.

**Further details on SBD approved products meeting the
Police Preferred Specification are available at:
www.securedbydesign.com**