IPVIEW SYSTEM SPECIFICATION

IPVIEW IP VISITOR VIDEO MONITOR DOOR ENTRY & RESIDENT ACCESS CONTROL. FULLY INTEGRATED, NETWORKED & CLOUD BASED SPECIFICATION 18/01/22

BATI CONNECT CLOUD

TOTAL 24/7/365 REAL-TIME REMOTE MANAGEMENT OF ALL YOUR SITES

IPVIEW® IP Video Entry

Secured by Design
SBD
Police Preferred Specification

1. Development specific communal visitor door entry & resident access control system equipment, operational strategy and drawings to be submitted for approval to both the client and the Design Out Crime Officer (DOCO) representing Secured By Design.

2. Building Control regulations always take priority over all Secured By Design requirements.

3. System and installation must comply fully with the Equality Act 2010 (DDA) to anticipate and prevent disability discrimination and so ensure that disabled persons receive a similar level of service provision as able-bodied persons.

4. System must comply fully with the Data Protection Act 2018, and the UK GDPR, and/or with subsequent legislation.

5. System must comply fully with the latest Secured By Design regulations for visitor door entry & resident access control.

6. No door, irrespective of its location, must open over a visitor door entry or resident access control panel.

7. Visitor door entry panel(s) must have passed the test as a critical component of a door set within the British security standard LPS1175 -SR2, and thereby achieved Secured by Design (SBD), Police Preferred Specification.

8. All visitor door entry panels and resident proximity access control panels (readers) to be vandal resistant with security screw fixings.

9. Visitor video door entry panel(s) must be IP Door Entry Ltd IPVIEW IP range, full IP/PoE, fully Equality Act 2010 (DDA) compliant. Keypad buttons for calling on panel to be alphanumeric, anti-vandal, tactile, raised and minimum 15mm diameter and with, on the button itself, braille for the blind and large minimum 8mm height illuminated LED digit/characters for the visually impaired.

10. IP Door Entry Ltd IPVIEW IP visitor door entry panel(s) serving communal entrances into a residential building must be equipped with integral anti-vandal colour/mono (day/night) high resolution camera(s) for Equality Act 2010 (DDA) compliance (visually impaired residents must be provided with a close up of the visitor calling), and every integral panel camera must meet the technical specification(s) as stipulated by Secured By Design. Written confirmation of panel camera specification is required.

11. IP Door Entry Ltd IPVIEW visitor door panel must be installed at 1.2 metres AFFL to its centre.

12. Resident only doors with proximity access control (reader) must be installed so that the proximity reader is fitted so that its top is 1.0 metre AFFL.

13. Resident proximity access control (readers) must be fully Equality Act 2010 (DDA) compliant; large, obvious (image of a key), bright, illuminated, and have LED's and buzzer to indicate authorised, declined and door open.

14. IP Door Entry Ltd IPVIEW IP visitor door entry systems must, for security reasons, provide full visitor call logging. The system must have the facility to identify the visitor calling panel (where the visitor made the call from), the time and date of the call, and whether the resident called opened the door. This is a Secured By Design requirement so that any resident abusing the system can be identified.

15. IP Door Entry Ltd IPVIEW IP visitor door entry panel(s) to include Equality Act 2010 (DDA) information voice output and visual display output messages for visitors.

16. A white Wi-Fi enabled handsfree 7" colour screen video monitor is to be installed at 1.2 metres AFFL to its centre in each flat. All visitor video calls to simultaneously auto-forward to smart phones / devices anywhere as determined and programmed by the resident of the flat. The quantity of fixed video monitors required may be greater than 1no per dwelling so the system must be capable of meeting such requirements. The resident can choose to answer, communicate with the visitor and grant access using the fixed video monitor(s) and/or smart devices.

17. The Wi-Fi enabled handsfree 7" colour video monitors can also make audio calls to other flats and the concierge (if applicable).

18. The Concierge station (if applicable) can make a video call to all flats Wi-Fi enabled handsfree 7" colour video monitors.

19. Sitewide resident access control systems will all be fully remotely programmable via BATCONNECT CLOUD based server. No software will be required.

20. Keypad code external door opening is not secure and cannot identify the code user. The system must, however, provide this feature for facilities staff.

21. Tradesperson time-zone programmable door opening buttons on visitor door entry panels are not normally permitted by Secured By Design. However, the IP Door Entry Ltd IPVIEW IP visitor door entry panel(s) must allow for this feature, because it may be specifically instructed because the main entrance door opens into a secure lobby where the post boxes are located.

22. All communal resident access control proximity readers for doors, gates, lifts, all IPKEYSAFE(s), and all radio access control receivers for vehicles on the development to be networked and fully remotely programmable via the BATICONNECT CLOUD based server. It must be possible to remotely connect into the sitewide access control systems to add or delete proximity key fobs, radio transmitters, keypad, and amend individual and/or group access rights to or from one, some or all doors, gates, lifts and change any system parameter.

23. For security compartmentalisation reasons and/or as requested by the Secured By Design DOCO for buildings of over 10no flats sharing a communal entrance, a "Meet & Greet" access control strategy may be required to achieve Secured By Design certification. Residents would usually "Meet & Greet" their visitor on the ground floor and then escort the visitor to their flat.

System must be capable of providing the following additional features, if requested:

- Each resident is issued with a unique proximity key fob that is programmed to only give access to their floor and any other communal areas relevant to them.

- Every lift must be floor specific proximity reader controlled.

- Every stairwell door onto a floor must be proximity reader controlled.

- Every ground floor communal stairwell door must be proximity reader controlled.

- Every corridor door leading to dwellings must be proximity reader controlled.

- Ground floor communal stairwell door with a secondary IP Door Entry Ltd IPVIEW IP visitor door entry panel with integral resident proximity access control, allowing the resident and visitor the option to "Meet & Greet" at the door from the stairwell onto their actual floor.

24. Each lift must be equipped with floor specific proximity access control that is an integral part of the fully and remotely programmable resident access control network. The lift proximity reader system feature means that the proximity key fobs issued to residents also only enable their specific lift floor button so as to restrict each resident to their floor only.

25. All communal doors, vehicle gates, barriers and lifts that provide a means of accessing into the housing development, into any block or core, onto any floor or corridor, into any car park, communal garden or allotment must be proximity reader and/or radio transmitter network access controlled.

26. All communal visitor ground floor internal lobby doors to be proximity reader networked access controlled. The objective is to create a secure lobby.

27. All communal bin, recycling and bike stores to be proximity reader networked access controlled.

28. All communal gardens, podiums and terraces must be proximity reader networked access controlled.

29. All communal vehicle gates and barriers to be networked radio transmitter access controlled for cars and networked proximity reader access controlled for cyclists. Both systems are to be on the same site wide access control network and fully remotely programmable.

30. The visitor door entry and resident access control system must have the facility to record and identify the location, user, type, time and date of every system event, and provide this information both in real-time and via remote data-retrieval. Sufficient memory storage must be available for a period of not less than 30 days.

31. Access control to the block(s) and carpark(s) by the residents is to be based on a fully integrated and networked proximity key fob and radio transmitter system. This is a requirement for Secured By Design 2014 onwards certification. Radio access control for vehicle gates is also a requirement for Equality Act 2010 compliance. The proximity key fob readers and radio transmitter receivers must be remotely programmable and provide a full log of all visitor and resident system events via the BATICONNECT CLOUD based server. No software will be required.

31. Proximity key fobs/cards/tags are to be security encrypted - minimum MIFARE Classic 13.56 Mhz technology, or MIFARE DESFire 13.56 Mhz. In addition, special security algorithm check protections are required to prevent access via duplicated credentials meaning copies/clones/forgeries. The same applies for radio transmitters. Access control systems which use proximity key fobs and/or radio transmitters that can be copied/cloned/forged by unauthorised parties are NEVER fit for purpose.

32. Older technology proximity key fobs, for example 125 Khz and 153Khz, are never acceptable.

33. Radio transmitters for vehicle entrances must also incorporate and utilise the rolling code security feature, transmission and reception.

35. Proximity key fobs and radio transmitters must each have a factory engraved visible unique ID number.

36. Quantities: 3no proximity key fobs required per plot, 1no radio transmitter required per secure carpark space (if applicable), plus 10% extras of both types. A printed list detailing the incremental sequential ID numbers of every proximity key fob and radio transmitter that have been supplied is required.

37. The access control strategy is based on the principle that a resident only needs to be issued with 1no proximity key and 1no radio transmitter which can be programmed via the BATICONNECT CLOUD to provide the exact door, gate, barrier and lift access authorisation profile for the entire development and, if necessary, for other remote developments. Master and facilities staff proximity key(s) and radio transmitter(s) must also be remotely programmable into all sites, any configuration as instructed.

38. All access controlled doors irrespective of location require, on the secure side, a double pole (PTM & PTB) green mushroom type exit button (or similar Equality Act 2010 compliant button) fitted within 1 metre maximum distance of the relevant door pull/push handle at a maximum height of 1 metre AFFL. The door must never open over the exit button. Additional press to exit buttons are to be installed, on the secure side, at distances of over 1 metre from the relevant door to facilitate exit for disabled persons in wheelchairs (as instructed).

39. All internal only fire route access controlled doors must be interfaced with AOV/FIRE alarm systems, as applicable. On alarm activation the 12/24V fail safe electric locking on the door must automatically and immediately fail safe (unlocked).

40. External doors that give access into the building from public areas are not to be interfaced with AOV/FIRE alarm systems unless instructed otherwise.

41. Green plastic emergency exit breakglass units are not permitted by Secured By Design on final exit doors - which are the external doors that give access into the building from public areas. Instead, a 2no stainless steel button (each min dia 30mm and DP) anti-vandal emergency exit system with self-resetting hold-open of 5 minutes and/or longer (Example: IP Door Entry Ltd ref. EM24EX) is to be installed and fitted within 1 metre maximum distance of the relevant door pull/push handle at a maximum height of 1 metre AFFL. The door(s) must never open over EM24EX exit systems. Technical submittal required to confirm that the emergency exit device installed is fit for purpose in relation to H&S requirements.

42. Door release exit buttons and other such devices used for exiting via vehicle entrances, pedestrian gates and bike stores must be carefully positioned so that they are not reachable from the public side whether by hand, stick or other object. If visible from the public side, the button itself must face in the opposite direction to the gate/door, be concealed or otherwise suitably protected from unauthorised activation, whilst remaining highly visible and easy to use by persons exiting. The door(s) must never open over door release exit buttons.

43. Full compliance with the building code is required to ensure guaranteed safe egress in the event of an emergency. Fire escape doors and routes must be clearly identified by others.

44. All electric locking supplied must have Secured By Design certification as part of a complete doorset (by the door supplier). Electric locking circuits must only use power cabling ref. 4 x 1 YY/LSZH per lock, or Fire Protected equivalent.

45. All cabling to communal visitor door entry panels, resident access control proximity readers, radio access control receivers, exiting devices, every locking device to be run on the secure side of the installation and concealed. Where cabling cannot be concealed it must be contained within metal conduit to prevent tampering. Accessible cable junction points on containment runs require security screw fixings on the covers.

46. Main control, programming and any recording equipment for the visitor door entry and resident access control systems must be housed in locked cabinets sited within secure internal locations.

47. All communal visitor door entry and resident access control equipment installed in risers or plant rooms must be housed integral to secure metal/steel cabinets and clearly marked. System equipment mounted directly onto walls without protective enclosures is totally unacceptable.

48. The resident access control system shall be supplied complete with own data modem(s) and communications package by the security specialist, and will include unlimited communications and BATICONNECT CLOUD programming access for a defined period starting from the point of handover.

49. Secured By Design requires that the communications package must be live at handover and full remote connectivity for the resident access control must be demonstrated as operational.

50. Both the builder and the security specialist are to liaise with the relevant Secured By Design DOCO and ensure compliance with the requirements of the latest edition of the Access Control section of Secured By Design, New Homes. Every scheme must comply with the latest Secured By Design guidelines.

51. The security specialist is to include for unlimited remote programming of proximity key fobs and radio transmitters, using the modem & BATICONNECT CLOUD communications package provided with the system for a defined period for each building starting from the point of handover. Residents must be able to purchase proximity keys and radio transmitters. Residents must be issued with a User Information Manual.

52. The security specialist is required to maintain, record and process all system and resident proximity and radio access control data as demanded by National Security Inspectorate (NSI) document NCP109.

53. The security specialist must attend concierge locations (as instructed) to demonstrate full remote access, programming and monitoring control for every block on every site reference all systems installed. All programming control to be available via the BATICONNECT CLOUD based server. No software is required.

54. Site specific "As Installed" visitor door entry and resident access control system drawings and strategy, together with operating manuals must be provided.

55. Objective of this Performance Specification is to make best use of modern technology to maximise performance and cost benefits, and to achieve consistency of visitor door entry and resident access control systems, equipment, strategy, operation and programming on all housing developments. This specification must be strictly adhered to. The visitor door entry, resident access control will be the IP Door Entry Ltd IPVIEW IP visitor entry system with BATICONNECT® CLOUD.

56. The builder, in conjunction with the security specialist, will issue a certificate to confirm that the visitor door entry and resident access control system installations and strategy comply fully with the requirements of this document.

57. The security specialist will issue a National Security Inspectorate (NSI) certificate to confirm full compliance with NSI document NCP 109.

58. Full ownership, with full access rights to the system, belongs solely to the Client reference the entirety of the systems, installations and programming.

IP DOOR ENTRY

08000 156496
sales@ipdoorentry.co.uk
www.ipdoorentry.co.uk
f in ipdoorentry

IP Door Entry Limited
Unit DC4 Prologis Park
Eastman Way
Hemel Hempstead
HP2 7DU

BATI CONNECT
CLOUD
24/7/365
www.baticonnect.com