datanet.co.uk Private Cloud Solutions

Out Of Hours (OOH) Access Conditions and Procedures – General

This security policy and procedure is to protect Aspen House Fleet, the property of our customers and DATANET.CO.UK. Your co-operation with this will ensure the safety and security of all concerned. DATANET.CO.UK will require your photo ID, car registration number and your response to a security question. Any changes to these details must be notified immediately to Datanet or access may be declined on arrival.

- 1. "Out Of Hours" (**OOH**) Access is available outside of normal support hours (9:00am to 5:30pm Monday to Friday).
- 2. OOH Access is by request a half hour in advance and only available if you are on the Authorised Contact list with AHF Out of Hours Access Permission.
- 3. Call Shield Security 30 minutes before OOH access is required. Shield Security 24 hour control room: 01252 319899, Mobile: 07836 696716, only call Shield Security for access during OOH.
- 4. On arrival you will be given your access card and you must sign in and out using the visitor's booking system.
- 5. You must carry your access card at all times. Shield Security will not provide spare or additional cards. When you leave, you must return the access card.
- 6. Shield Security will check you against the access list and ask a challenge question from the list, you must ensure your details are up to date on the list.
- 7. If your business demands you bring a visitor to site, they must sign in and out using the visitor's booking system and must wear a visitor badge and be escorted at all times. You are responsible for your visitor's Health & Safety, Security and ensuring the terms of the Confidentiality & Non-Disclosure Agreement are met.
- 8. When you are finished on site, call Shield Security, advise them you are leaving site and request they attend site to do a full alarm set and lock, do not leave the building un-attended (note: CMC060810 if you need to leave the building for a short while e.g. 20 minutes to get a sandwich, please call Shield and advise, they will monitor the cameras more vigilantly until you return).
- 9. The inner front door and lobby area have security grilles in place. Please ensure the doors close firmly behind you.
- 10. The rear fire doors (ground and first floor) and the rear double delivery doors are monitored on a 24 hour alarm basis and will sound an internal sounder if activated, the internal sounders are located near racks C27/D27 and adjacent to the rear fire doors at each level (3 sounders). If you want to open the rear fire doors or delivery doors you must ask a keyholder or Shield security to disarm the system (green light). Keyholders, you are responsible for disarming and ensuring the system is rearmed (no light) in a timely fashion. In the event of a fire all these doors will open when you press the emergency "break glass" buttons, remember too on the outer front door to turn the fail secure lock, please ask a key holder to demonstrate this to you.
- 11. If the doors are forced the internal alarm will sound as above, you will have to ask a keyholder to reset the system, if it happens out of hours and you are on your own in the building there may be an intruder so call shield security on 01252 319899 or the Police on 999 if you believe there is a real security risk.
- 12. If you require Technical Support from Datanet during OOH, please call the usual 24 hour support number 01252 813396 stating your business name.
- 13. If you require any other emergency assistance on site, please call Dave Smith on 07525 193641 or Conleth McCallan on 07973 113586.
- 14. Personnel requiring OOH Access must first attend a Health & Safety briefing here at Datanet during which time they will sign a Confidentiality & Non-Disclosure Agreement and we will produce their Photo ID for future visits.
- 15. Datanet require one clear business day to make deletions or changes to the Authorised Contact List, this must be requested by a Company representative (Authoriser).
- 16. Digital images are recorded throughout the facility and stored for approximately 90 days. Shield Security and Key Datanet staff monitor these remotely.