CPNI

Centre for the Protection
Of National Infrastructure

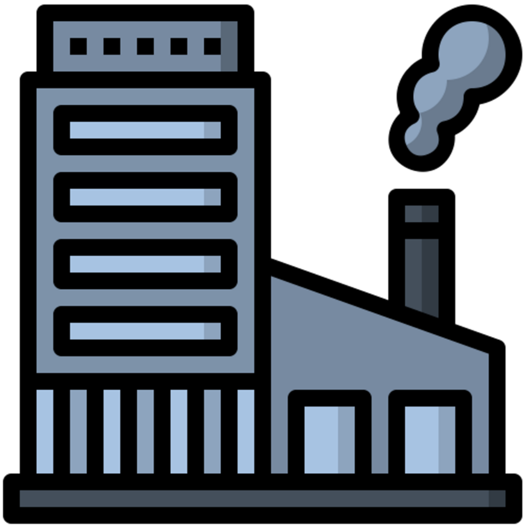
Automatic Access Control and COVID-19

1. Pin pads and biometrics should remain in operation. They should be highlighted as “touch points” and cleaned regularly – they are touched less than door handles!

2. AACS proximity cards will work up to 10cm from the reader – there is no need to physically touch the card on the reader.

3. Staff should be reminded not to put passes into their mouth i.e. when removing from bags

4. AACS cards should be highlighted to staff as “touch points” and should be cleaned regularly.



5. Tiger traps and pods can be “vented” by opening the inner door – however this will reduce the attack delay

ONE door should always remain closed to maintain security

6. Balance the number of exits / entrances open as work force and guard force numbers vary and staff return to a partially locked down building.

7. AACS cards are not identification cards and if AACS is not being used, other formal, government issued, identification should be used. These should be passed through a security screen or an ‘ajar’ car window to a security officer for checking. While it is not necessary to clean each document, staff handling documents should have hand sanitiser, gloves or regular hand washing breaks

8. Queues need to be carefully managed:

- inside the building for social distancing
- outside the building for social distancing and security as queues (in the initial return to work stage) will be key workers and may be an attractive target

9. Cleaning should be increased as lockdown is eased, and footfall is increased.

10. Staff should be reminded of their ongoing security arrangements around passes. During lockdown, staff are away from the office for a significant time. They should still be aware of their site pass and hold this securely.

11. Intercoms should also be highlighted as likely points for contamination and should be cleaned regularly.

12. Hand sanitiser should be placed in convenient locations to allow occupants to clean their hands after interacting with AACS measures

13. AACS cards are like smartphones, memory up to 32kb which contains applications. Each app (i.e. AACS) will have its own ‘keys’. These need to be protected and held by the site. AACS manufacturers should not be looking after the keys to sites.

CPNI

Centre for the Protection
Of National Infrastructure

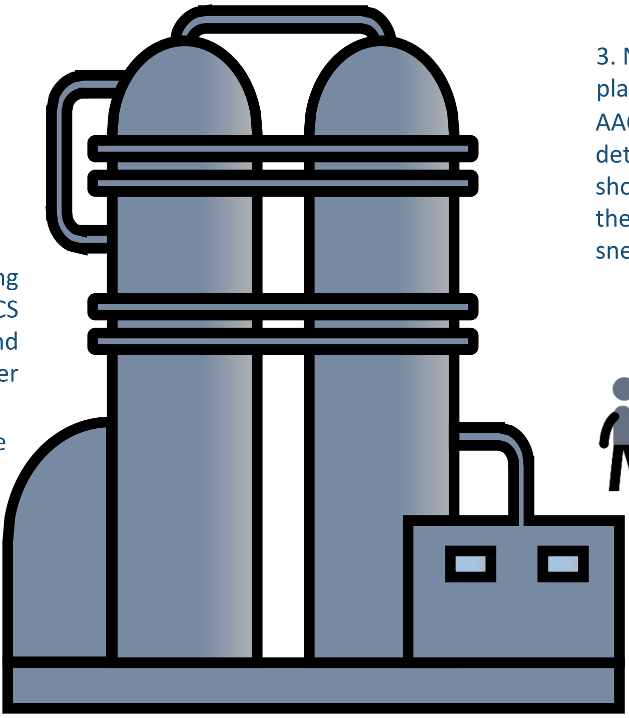
Automatic Access Control and COVID-19

1. Physical keys should be cleaned before and after each issue. Sanitiser or wipes should be provided at the issuing location

2. The number of people within a “tiger trap” should be limited and social distancing met. Tiger traps will have fewer people in but should continue to be used.

8. Adjusting working times may reduce the peak flows into the building.

3. Notices should be placed close to any AACS measures, providing contact details for cleaning teams. Staff should be briefed when to contact the cleaning teams i.e. when sneezing inside an AACS pod



7. It is likely that during the lockdown period AACS rights will be altered and changed in a rapid manner a defined period should be set for review of these new rights and time should be set aside for “admin consolidation” once lockdown is eased.

4. Staff induction should include detail on AACS security – see CPNI AACS video on YouTube

6. AACS system may have a “time out” feature, passes will automatically lock out if not used for 30 days. Sites should expect when staff return from lockdown, they will need to process a larger number of “pass renewals”

5. New technology can assist with the reduction of touch points, push to exit buttons can be replaced with IR “buttons” or, better still, card readers - (increasing security AND reducing touch points) and doors can be motorised (assisting those with mobility issues AND reducing touch points)

9. AACS will be able to provide a good solution to know who was in your building and where they went when lockdown measures be relaxed.

If population tracking is required, AACS may be able to provide a log of a persons whereabout and who they were in close proximity to.

10. While supply chains might be disrupted, it may be sensible to increase the number of on-site spares held.

11. Remote dial in for maintenance of is an option during the lockdown phase. But it should be noted that the number of cyber-attacks relating to the COVID pandemic has been high.

Use good IT practice (such as VPN) and see CAPSS guidance