



MAINTAINING OPERATIONAL EXCELLENCE

Site access assurance policy & principles



Establishing the policy and principles around access to Cornerstone sites

The following document sets out the policy and principles around access to Cornerstone sites.

Cornerstone is responsible for the safe access, egress, build, upgrade, maintenance, structural integrity and security of over 16,500 sites. We have a duty of care to all visitors, which is why it is crucial that we uphold the highest safety standards.

By providing up-to-date, site-specific health and safety information, maintaining operational control and visibility of all site activity, and implementing an accreditation process that ensures only competent personnel are granted access to our sites, we protect personal safety and site security. These measures also safeguard our integrity and help us maintain operational excellence.



ENSURING SAFE AND CONTROLLED ACCESS ACROSS OUR ESTATE

Site access assurance principles



Cornerstone is committed to ensuring the safety of people and infrastructure on our estate by establishing:



ESTABLISHING A STRONG FOUNDATION FOR SAFETY

- Robust operational controls
- Providing up to date site specific health and safety information
- Monitoring, measuring and governance



IMPLEMENTING EFFECTIVE CONTROLS AND COMPLIANCE

- Managing all access via Locken Notification of Works (NOW)
- Accreditation process for organisations and individuals
- Providing site specific hazards and risks via the NOW booking system
- Managing any breaches of access
- Conducting compliance audits and performance reporting

Access management

Access to Cornerstone sites must always be planned in accordance with the latest access information and via Cornerstone MyLocken.



All visits to Cornerstone sites must be booked by raising a NOW (Notification of Works) via the Cornerstone MyLocken app.



Cornerstone has installed Locken smart locks across the estate. These locks are designed to improve site safety and security by giving access only to permitted users and providing an audit trail of site entry.



All NOW bookings must accurately reflect the nature of the works to be undertaken.



All access must be planned and undertaken in accordance with the Access Notes for the site and these must be checked prior to accessing the site, bearing in mind these are subject to change.



All site visits are to be planned to take account of the published residual hazards for the site.



All site visitors must ensure that the site environment and relationships with neighbours and local site providers are responsibly managed.



Any suspected misuse will be dealt with using the Site Access Breach Management Process.



Activities requiring additional approvals

Health and Safety documentation will need to be uploaded when submitting a request, for example, Risk Assessments, Safe Systems of Work and Construction Phase Plans. Some sites may need the documentation to be reviewed prior to access being granted. In these circumstances the documentation required must be uploaded within any agreed time frames to allow for effective planning and review. These sites will be identified as part of the booking process, some examples of which are opposite. The approval of Risk Assessment & Method Statements (RAMS) is managed via the Halo portal.

In the event of a specialist contractor being requested to carry out works as a one-off visit, the sponsoring company/contractor must request access and oversee these works in a principal contractor capacity. The NOW booking must clearly state the description of works.



WORKING AT HEIGHT

- Working from a man-basket
- Rope access
- Complex bespoke scaffolding solutions requiring a design
- Near overhead power lines



ELECTRICAL WORKS

- Works on high voltage substations
- Any access to G78 pylons
- Live working



LIFTING OPERATIONS (COMBINATION OF 3 OR MORE)

- Large, prefabricated steelwork
- Mobile elevated work platforms
- Traffic and pedestrian management
- Use of derricks
- Tower builds
- Capstan winch
- Helicopter lifts



EXCAVATIONS

- Large plant and equipment
- Traffic or pedestrian management required



NEW SUPPLIER ON MYLOCKEN (TIME PERIOD)



RAILSIDE INFRASTRUCTURE REQUIRING BAPA



TEMPORARY WORKS



SITES WITH STRICT SAFETY PROTOCOLS



NEAR WATER COURSES



SAFETY CONCERNS AND SITE ISSUES

Hazard and incident reporting

Any issues identified on site must be reported as follows:

- Accidents, incidents and near misses: via **Halo portal**
- Facilities issues, such as overgrown vegetation, broken locks or minor damage via Facilities Helpdesk **01329 332844** or **01329 332846** or alternatively email us at **Cornerstone.Servicedesk@mitie.com**
- Site Access Issues such as landlords being unavailable or not permitting access to site **www.cornerstone.network/report-site-issues**

PROCESS FOR SITE ACCESS AND COMPETENCE

Site access assurance accreditation

Cornerstone is committed to ensuring the competence of companies and individuals accessing Cornerstone sites.

From Spring 2025, Cornerstone shall require all Tier 1 suppliers to be Alcumus Safe Contractor accredited, and to nominate and manage their appointed subcontractors appropriately and ensure they are suitably competent.

All companies registered with Cornerstone must nominate a primary point of contact for all communications, audits, and investigations.



COMPANY ACCREDITATION PROCESS

Where Alcumus Safe Contractor Accreditation is held, evidence of this will be required on an annual basis. Cornerstone will regularly review this and any revocation of Safe Contractor accreditation will be subject to review by Cornerstone.



Site access requests

All access to Cornerstone sites must be pre-booked via the Cornerstone MyLocken app and must accurately reflect the nature of the works to be carried out on site.

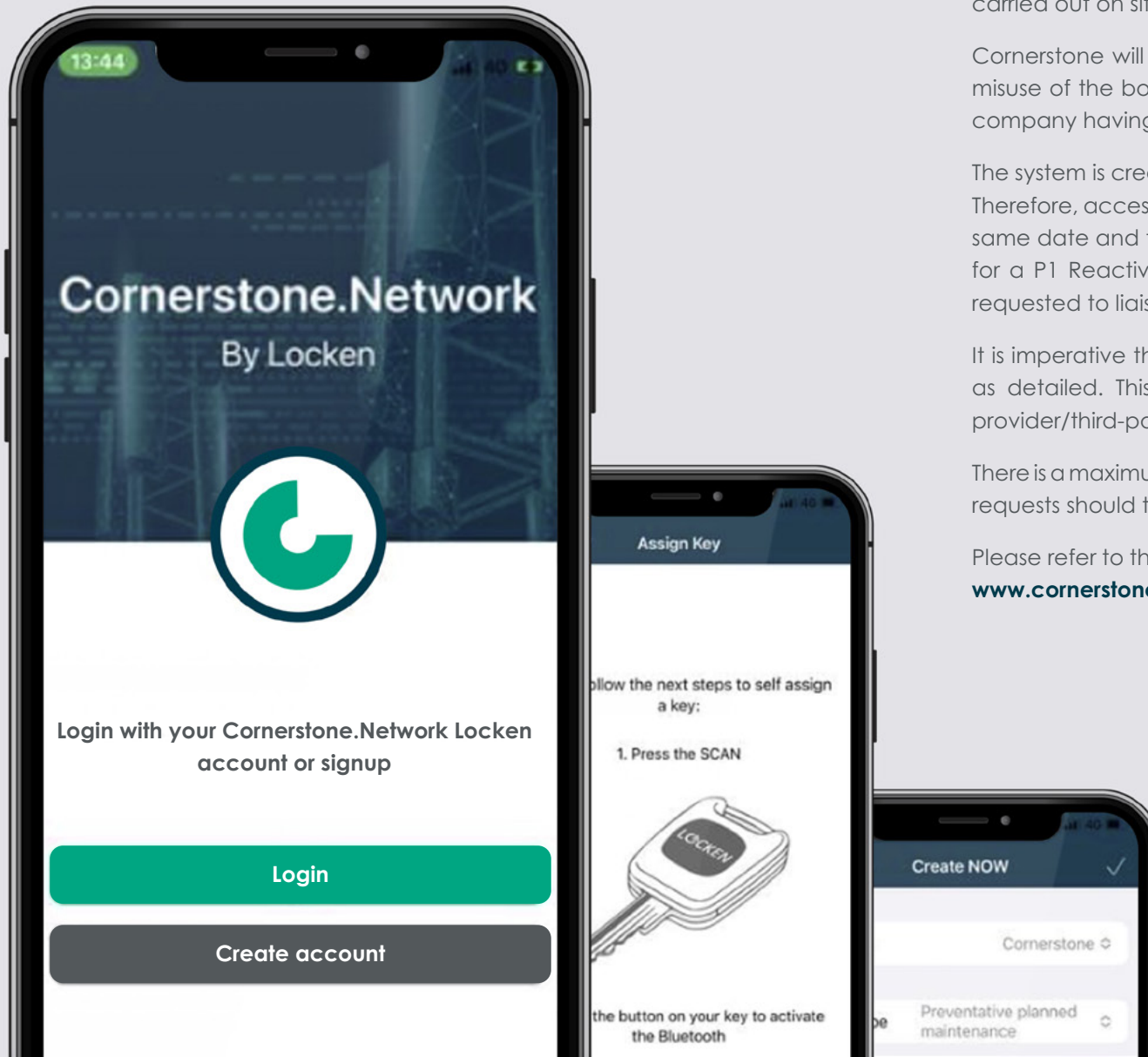
Cornerstone will perform audits on access booking and will investigate any misuse of the booking system. This may result in users and/or the accredited company having their access revoked.

The system is created to ensure the safety where possible of visitors to the site. Therefore, access shall not be permitted where a site is already booked for the same date and time. There shall be an exception where access is requested for a P1 Reactive Fault and in this case, both parties shall be notified and requested to liaise to ensure safe access for both parties can proceed.

It is imperative that the Access Conditions for each site are followed exactly as detailed. This includes obtaining any required notice periods and site provider/third-party approvals, and adhering to all access restrictions.

There is a maximum booking period of 5 days for any access request. Additional requests should therefore be submitted for any works exceeding 5 days.

Please refer to the Locken User guide and additional information available at www.cornerstone.network/site-access-management



Key management

The following section details the processes and principles around the use of Cornerstone issued keys, including Locken keys. For further guidance on the use of Locken keys, including troubleshooting, and the raising of NOWs, please refer to www.cornerstone.network/site-access-management

For BAU key queries please contact key.requests@cornerstone.network

KEY MANAGER RESPONSIBILITY

Each company/organisation will ideally have two named representatives, a primary and secondary key manager. The primary key manager will have complete responsibility for all keys requested by and issued to personnel within their company or to other companies acting/undertaking work on their behalf. The secondary key manager is a point of contact if the primary key manager is on leave/absent.

By submitting a key request, the requester is acknowledging they have read, understood, and agreed to SDN 2006 and the Terms and Conditions contained within the request form.

The requester is assumed to be authorised by their company.

TRANSFER OF KEYS

Transfer of key ownership should be informed by the completion and submission of a Transfer of Ownership request in the **Halo portal** detailing the former engineer's name, and the related key serial number.

Key sets will be issued in relation to the related works/Project activity, any additional key sets above the agreed key set volume for the works/project may be chargeable.

It is the responsibility of the Key Manager/Company to ensure that all certification for engineers/employees/contractors is in date.





APPLICATION FORMS & APPROPRIATE USE

Key management

KEY APPLICATIONS

The Cornerstone Locks, Keys, Signage application request is in the form of an Online portal controlled by Cornerstone.

The link to the portal can be found at: **Halo portal**

We will endeavour to fulfil requests which are accurate, complete, and where all approvals have been provided, as soon as possible but Orders can take up to 25 working days to procure. Where applicable, if an order requires a Purchase Order Number, the order shall not be considered in progress until the Purchase Order Number has been received and updated within the ticket that has been provided when the request was made.

APPROPRIATE USE & MANAGEMENT OF KEYS

All Cornerstone issued keys must be kept safe and secure at all times.

Keys must only be used by the organisation to whom they have been issued.

Individuals must return their keys to the organisation they are registered to on the termination of their employment.

Any misuse of keys will result in them being suspended and could result in the user's account and/or accreditation being revoked.

Locken keys must be looked after appropriately, bearing in mind these are not as resilient as a traditional mechanical key. It is the key holder's responsibility to manage the battery level of these keys. Keys which have been lost, stolen or broken must be reported to Cornerstone via the online **Halo portal**

LOST OR STOLEN KEYS

Cornerstone considers a loss as negligence. Cornerstone estate keys not only hold significant value but also provide access into areas that are considered business critical, thus lost keys render the estate vulnerable and insecure. Any Locken key identified as lost or stolen must be reported to Cornerstone via the **Halo portal** then Cornerstone will then ensure this key is deactivated.

STOLEN OR SNAPPED KEYS

Key management

LOST KEYS

Any keys reported as lost will be charged to the Company in charge. There is no exception to this and by acknowledging you have read and understood this document when submitting the key application form, you are entering into the agreement for your Company.

STOLEN KEYS

A Police Crime Reference Number must be provided for any keys reported as stolen from a secure building. Keys stolen from a vehicle (whether locked or not) or whilst on site will be considered negligent. A fee may be charged to the company who requested the keys. Lost or stolen keys will be invoiced at the current replacement cost. If any keys are lost, stolen (other than from a secure building) or unaccounted for, Cornerstone may invoice the company. If payment is not received the Company may be restricted from further keys being issued until payment is received.

SNAPPED KEYS

Any mechanical key that snaps will be replaced free of charge. A new key application must be submitted for the engineer with a supporting photograph of the snapped key. Some keys have their own serial number inscribed into the key; a photograph of this serial number should support a new replacement. If a Locken key has been reported as snapped/ broken, please report these issues for deactivating at the earliest opportunity. The snapped Locken key will be required to be returned to Cornerstone. If misuse is suspected, Cornerstone may charge for a replacement to be issued. Both mechanical and Locken keys that have been snapped, must be reported to Cornerstone via the **Halo portal**

RETURN OF KEYS

Keys which are no longer required should be returned to Cornerstone's key supplier at the key holder's expense and a signature obtained for their delivery. Email cornerstone.locks.keys.signage@mitie.com for details of the process.

AUDITS

Periodic audits will be carried out by Cornerstone or via it's representative, on any companies who have requested and hold Cornerstone issued keys. All keys must be accounted for within 14 days of receiving the audit request. Any keys unaccounted for at the end of the 14 days will be considered lost and may be invoiced for as per Section 6. It is, therefore, the responsibility for each company, to keep accurate records.



ON-SITE EXPECTATIONS

Environment, neighbours and local site providers

Cornerstone is committed to ensuring good relationships with its site providers and neighbours. All site visitors are required to behave responsibly, respectfully and in accordance with the access Information provided.

Any damage caused on site must be made good by the visiting organisation, to the satisfaction of Cornerstone and the site provider. It is important to ensure that sites are left tidy and secure.

The following behaviours will not be tolerated (please note this list is not exhaustive):

01

Access routes must be adhered to, including driving at an appropriate speed, adhering to any speed limits and not blocking any driveways.

02

Ensuring access routes are kept clear and lights switched off on exit (as appropriate).

03

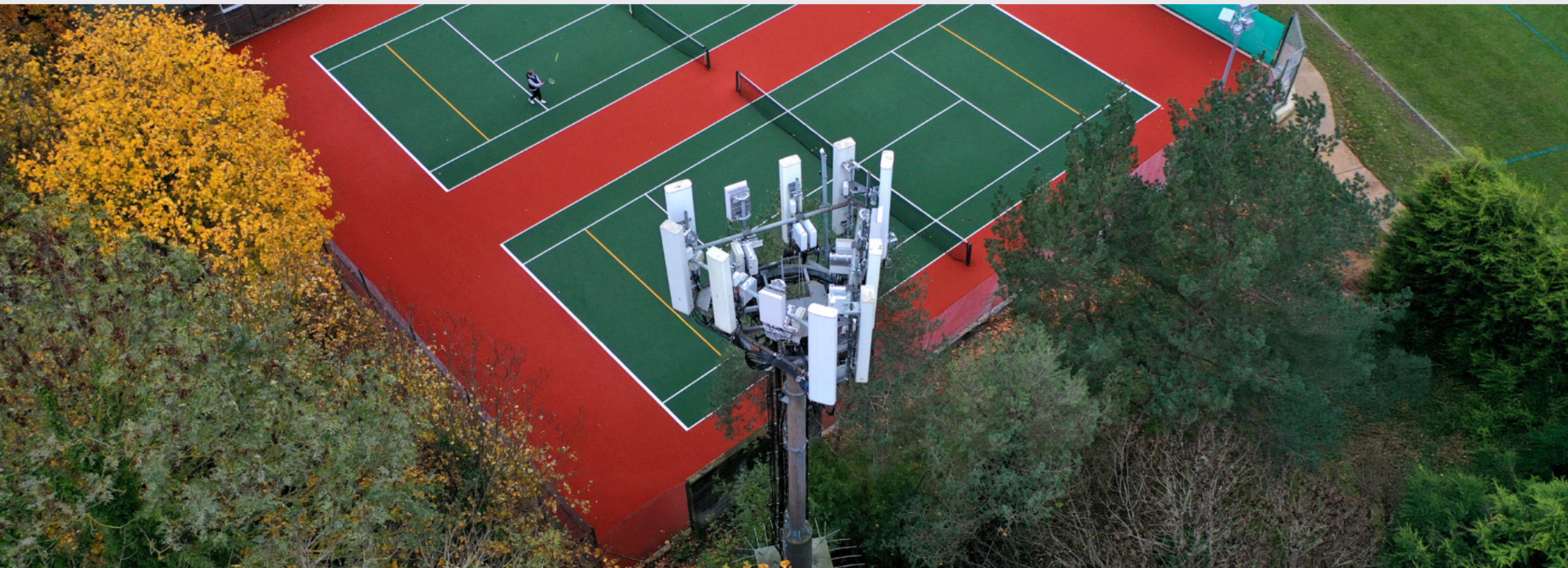
Causing physical damage or degradation to land either on the permitted access route or elsewhere on site.

04

Leaving litter or waste materials on site.

05

Shouting and the use of offensive language.



PROCEDURE FOR ADDRESSING SITE ACCESS VIOLATIONS

Breach management process

The following process will be applied in the event of breaches of this Site Access Assurance Standard Document and to help ensure Cornerstone maintains safe, secure sites with good site provider relationships.

Each instance of breach will be fully investigated and an explanation sought, as well as the measures to minimise any recurrence. All breaches will be logged, and subsequent breaches may result in a more severe outcome.



Breach received and reviewed by Site Access Assurance Lead.



Company and instructing party informed; explanation and remedial actions requested. Sponsoring party may also be notified.



Response reviewed.



Follow up actions agreed and company advised.

Companies with persistent breaches will be closely monitored, and the following actions may be taken:

1. Meeting to discuss the root cause of these incidents
2. Appointing party/supplier notified
3. Individual users access suspended
4. Company's access revoked and prohibited from accessing Cornerstone sites

Issue management

Any changes to access information, or issues related to gaining access to the site, such as a Site Provider's details changing or access being denied should be reported to Cornerstone. It is imperative to ensure these issues are promptly reported to keep our information accurate and up to date.

Routine, non urgent issues can be reported via **www.cornerstone.network/site-reporting** and any urgent issues reported via your customer interface/ remedy.

All cases should be reported providing as much detail as possible to allow the incident to be suitably managed.

SITE ACCESS ESCALATION PROCESS

Cluttons, on Cornerstone's behalf, will provide first line triage of reported incident. This incident will then be managed as appropriate to resolution. All cases must be reported via the correct channels as detailed above.

Cornerstone will ensure the appropriate management of all incidents but the below escalation path exists.

STAGE 1

Reporting of the issue via web portal/interface

Should an appropriate/timely response not be received please contact:

STAGE 2

Adam Hyams, Associate Cluttons

adam.hyams@cluttons.com 07725 960070

STAGE 3

Micaela Santos, Site Access Operations Project Manager

Micaela.santos@cornerstone.network 07795 612697

STAGE 4

Fran Jones, Site Access Assurance Manager

Fran.jones@cornerstone.network 07557 325471





Site Access Management - Cornerstone

