



Marking table for Access Control Systems installed to NCP 109 (Issue 3)

NSF 271 - Issue 2

June 2021

This marking table is for use by NSI when inspecting access control systems that have been installed by NSI NACOSS Gold and NSI Systems Silver approved companies to the requirements of NCP 109 (Issue 3).

Demerit points may be given for non-compliance with clauses of NCP 109 (Issue 3) for which no specific reference has been made in the table of deviations listed in this document

National Security Inspectorate
Sentinel House,
5 Reform Road
Maidenhead
SL6 8BY
Website: nsi.org.uk

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 1 of 10 | |

NCP 109 (Issue 3) marking table

The NCP 109 (Issue 3) marking table is divided into Sections A to L as listed below.

| Section | Title | Maximum points |
|---------|----------------------------------|----------------|
| A | Documentation | 1 |
| B | Handover and training | 1 |
| C | Equipment selection | 2 |
| D | Safety requirements | 2 |
| E | Security requirements | 2 |
| F | Environmental protection | 1 |
| G | Cable installation | 1 |
| H | Reader functions and indications | 2 |
| J | Access point hardware | 1 |
| K | Power supplies | 2 |
| L | Maintenance | 2 |

Notes

- Each deviation in this marking table is given a clause reference (for example 5.1), a Code (for example D2) and a Point score (for example 2 points).
- NSI Inspection Reports detail deviations by Clause, Code, Description, Points.
Example: NCP 109: 5.1 Access point(s) conflict with Building Regulations and/or Fire Safety regulations - 2 Points
- Points are awarded for each individual deviation as shown in the marking table. However, the maximum points awarded in any section are shown above.
Example: If two deviations D2 (2 Points) and D3 (2 Points) are raised under Section D (Safety requirements), a total of 2 points (not 4 points) is awarded against Section D.
- The total number of points awarded results in a grading (A to E). A = 0 points, B = 1-2 points, C = 3-5 points, D = 6-8 points and E = 9 points or more.

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 2 of 10 | |

The access control system will normally require a re-inspection if Grade D or E is achieved.

| Clause | Code | Deviation | Points |
|-------------------------|------|--|--------|
| A. DOCUMENTATION | | | |
| 4.2 | A1 | No evidence a risk assessment has been completed and/or risk assessment not documented. | 1 |
| 4.2 | A2 | Risks identified in the documented risk assessment are not addressed in the system design and/or not notified to the customer | 1 |
| 5.1 | A3 | No evidence the aspects (where applicable) detailed in the Code of Practice have been considered in the risk assessment and/or system design proposal. | 1 |
| 5.1 | A4 | Required methods to release access points in the event of an emergency not included in the system design proposal and/or as-fitted document | 1 |
| 6.2 | A5 | Existing or customer provided hardware associated with each access point that may require attention or action by the end user not documented in the risk assessment. | 1 |
| 7.2 | A6 | Responsibility for providing critical updates to system firmware and/or software not defined in the system design proposal and/or as-fitted document | 1 |
| 7.2.1 | A7 | No evidence customer permission was granted, prior to the connection of external devices (e.g. laptop, memory stick) to the customer's network. | 1 |
| 7.2.1 | A8 | No evidence external devices (e.g. laptops, memory sticks) have latest anti-virus software and/or operating system updates. | 1 |
| 8.1 | A9 | No evidence permission to retain user account details for ongoing maintenance provided by the customer and/or permission not documented. | 1 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 3 of 10 | |

| Clause | Code | Deviation | Points |
|---------------------------------|------|--|--------|
| 8.2 | A10 | Facility to record system events does not exist (e.g. electronic event log or system logbook). | 1 |
| 8.2 | A11 | No evidence the customer has been advised of their legal responsibility to comply with the DPA and GDPR in relation to the Access Control System. | 1 |
| 8.2 | A12 | The correct NSI certificate not issued within one month. | 1 |
| 8.2 | A13 | Details of remote management for the access control system not included in the system design proposal and/or as-fitted document. | 1 |
| 8.3 | A14 | No evidence of an accepted system design proposal and/or system design proposal does not include the required information. | 1 |
| 9.1.1 | A15 | No evidence customer was advised to take out a maintenance contract to ensure access points controlling access to/egress from emergency exits are maintained in working order. | 1 |
| 9.4.2 | A16 | No evidence that an as-fitted document has been completed. | 1 |
| B. HANDOVER AND TRAINING | | | |
| 8.2 | B1 | No evidence the customer was made aware of how to report issues that require attention. | 1 |
| 8.2 | B2 | No evidence that customer purchased software and/or software licenses were provided to the customer. | 1 |
| 8.2 | B3 | No evidence the customer has received training in the operation and maintenance of the access control system. | 1 |
| C. EQUIPMENT SELECTION | | | |
| 5.1 | C1 | Common system components are not of the same or higher class as the defined highest class of each associated access point. | 2 |
| 6.1 | C2 | Control equipment does not meet the required functionality to meet the risk assessment or the system design proposal. | 2 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 4 of 10 | |

| Clause | Code | Deviation | Points |
|---------------------------------|------|--|--------|
| 6.2 | C3 | No evidence the physical strength of access points has been taken into account. | 1 |
| 5.3.3 | C4 | For class 3 & 4 access points the release times are not configurable for each access point. | 2 |
| 4.3 | C5 | The class level for credentials are of a lower class than the defined classification for the access point. | 2 |
| D. SAFETY REQUIREMENTS | | | |
| 5.1 | D1 | The means to release electronically secured doors do not meet the recommendations of BS 7273-4. | 2 |
| 5.1 | D2 | Access point(s) conflict with Building Regulations and/or Fire Safety regulations. | 2 |
| 5.1 | D3 | Access point(s) restrict safe egress endangering persons in the case of an emergency. | 2 |
| 5.3.5 | D4 | No free exit when the access control system receives an override trigger from an emergency system. | 2 |
| 6.4 | D5 | Equipment housing not displaying the operating or supplied voltage | 2 |
| 7 | D6 | No evidence guidance has been obtained from fire door set manufacturers, when fitting access point hardware (including locks, latches and locking plates) to fire door sets. | 2 |
| 7.1.1 | D7 | Cables that are part of the 'critical signal path' do not meet the requirements of BS 7273-4. | 2 |
| E. SECURITY REQUIREMENTS | | | |
| 5.3.2 | E1 | Class 4 access point(s) do not include anti-passback with override or disablement. | 2 |
| 5.3.2 | E2 | Class 3 or 4 access point(s) are defined but credential expiry date is not included. | 2 |
| 5.3.4 | E3 | For class 3 & 4 access points the Secure state not monitored and/or access point held open not monitored and/or door forced not monitored. | 2 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 5 of 10 | |

| Clause | Code | Deviation | Points |
|---------------|------|---|--------|
| 5.3.6 | E4 | Central control equipment not installed in a secure location and/or does not have means to notify users when tampered with. | 2 |
| 5.3.6 | E5 | Access point equipment that can be accessed from outside the controlled area is not provided with adequate tamper protection. | 2 |
| 5.3.6 | E6 | Access point reader(s) configuration settings are visible externally when installed. | 2 |
| 5.3.6 | E7 | Access to system administration is available without the use of valid credentials and/or default ACS passwords were not changed. | 2 |
| 5.3.6 | E8 | Users have access to perform functions beyond their hierarchical role. | 2 |
| 5.3.6 | E9 | Data encoded in tokens or cards can be changed without the need for user authorisation. | 2 |
| 5.3.6 Table 6 | E10 | For class 2 access points and above, opening of an enclosure is not detected. | 2 |
| 5.3.6 Table 6 | E11 | For class 4 access points, communications between the access control unit and the access control system is not monitored. | 2 |
| 5.3.6 Table 7 | E12 | For class 2 access points and above, access to components does not require the use of a tool. | 2 |
| 5.3.6 | E13 | Access to biometric reader adjustment is not restricted to authorised users. | 2 |
| 6.4 | E14 | Power supply unit(s) supporting fail unlocked hardware not provided with additional security. | 2 |
| 7.2 | E15 | Appropriate measures are not in place to prevent local or remote access to the system or customers network by unauthorised users. | 2 |
| 8.1 | E16 | Unused user accounts have not been deleted or disabled. | 2 |
| 4.3 | E17 | The RFID reads the Chip serial number. | 2 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 6 of 10 | |

| Clause | Code | Deviation | Points |
|------------------------------------|------|--|--------|
| 5.3.6 | E18 | The access control system does not automatically restart on reinstatement of its power source and/or a trouble condition is not notified of failure of automatic re-instatement. | 2 |
| 5.3.6 | E19 | Access point(s) do not remain secure on failure or restoral of communications with any CIE. | 2 |
| 5.3.6 | E20 | Failure of communication between the central control equipment and access point controller(s) prevents the operation of access decisions. | 2 |
| F. ENVIRONMENTAL PROTECTION | | | |
| 6.3 | F1 | Equipment will not withstand the defined environmental temperatures. | 1 |
| 6.3 | F2 | Environmental housings are not classified according to BS EN 60529. | 1 |
| 6.3 | F3 | Equipment housings do not prevent the insertion of solid objects larger than 1mm. | 1 |
| 6.3 | F4 | Equipment housing(s) do not offer appropriate protection against impact damage. | 1 |
| G. CABLE INSTALLATION | | | |
| 7.1.1 | G1 | Cables do not meet manufacturers' recommendations and/or are not capable of supporting the electrical load. | 1 |
| 7.1.1 | G2 | Cables are not mechanically protected against tamper and/or damage. | 1 |
| 7.1.1 | G3 | Extra low voltage cable joints not made in suitable junction boxes using either soldered, crimped, or screw-terminals. | 1 |
| 7.1.1 | G4 | Extra low voltage cables are not segregated from low voltage cables and/or do not have an appropriate insulation rating. | 1 |
| 7.1.1 | G5 | Wiring not adequately supported. | 1 |
| 7.1.2 | G6 | Data cables are not adequate to support the electrical load or transmission rate. | 1 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 7 of 10 | |

| Clause | Code | Deviation | Points |
|--|------|--|--------|
| 7.1.2 | G7 | Test results for UTP network cabling were not available. | 1 |
| 7.1.2 | G8 | Data cables were not labelled clearly at each termination point. | 1 |
| 7.1.3 | G9 | Extra low voltage and/or low voltage cables are not of a sufficient size to support connected equipment over the length of the cable run. | 1 |
| H. READER FUNCTIONS AND INDICATIONS | | | |
| 5.3.7 | H1 | Access granted or denied event not visually or audibly indicated at the access point. | 1 |
| 5.3.7 | H2 | Central indications or annunciations are not available as required for each class of access point. | 1 |
| 5.3.6 | H3 | Visual and/or audible indications of keystrokes are distinguishable from each other. | 2 |
| J. ACCESS POINT HARDWARE | | | |
| 6.2 | J1 | Access point hardware does not provide the required performance or functionality to meet the needs of the risk assessment or system design proposal. | 1 |
| 6.2 | J2 | Manual emergency release controls are not distinguishable from fire alarm call points | 1 |
| 6.2 | J3 | Closing devices do not close and/or lock the door under normal operating conditions. | 1 |
| 7 | J4 | Access point reader(s) are not mounted securely in position. | 1 |
| 7 | J5 | Access point reader(s) are not mounted adjacent to their access points and/or convenient for all users including those with disability. | 1 |
| 7 | J6 | Access point hardware is not installed to avoid injury | 1 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 8 of 10 | |

| Clause | Code | Deviation | Points |
|--------------------------|------|---|--------|
| K. POWER SUPPLIES | | | |
| 6.4 | K1 | Power supplies will not support the largest load likely to be placed upon them under normal operating conditions. | 2 |
| 6.4 | K2 | Manufacturer's recommendations for use of power supplies were not followed. | 1 |
| 6.4 | K3 | Power supply unit(s) are not installed within controlled area and/or are not positioned to avoid tampering. | 2 |
| 6.4 | K4 | Mains power supplies are not fed from a dedicated unswitched fused spur. | 1 |
| 6.4 | K5 | Extra low voltage cables enter power supply enclosure through same entry point as mains cables. | 1 |
| 6.4 | K6 | Standby power supplies (if specified) do not have the necessary capacity to support the ACS for the minimum time period agreed. | 2 |
| L. MAINTENANCE | | | |
| 9.1.1 | L1 | Where a maintenance contract is in place, no evidence the company have the capability to maintain the ACS (e.g. access to spare parts, documentation etc.). | 2 |
| 9.1.2 | L2 | Service technicians do not have access to appropriate tools and equipment to maintain the ACS. | 2 |
| 9.2.1 | L3 | Preventative maintenance visits not carried out every 12 months from the date of commissioning. | 1 |
| 9.2.2 | L4 | No evidence the required preventative maintenance checks were carried out. | 1 |
| 9.2.2 | L5 | No evidence corrective action(s) identified during a preventative maintenance have been carried out in agreement with the customer. | 1 |
| 9.2.2 | L6 | Preventative maintenance checks and/or corrective action not completed not documented and/or no evidence agreed with the customer. | 1 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 9 of 10 | |

| Clause | Code | Deviation | Points |
|--------|------|---|--------|
| 9.3 | L7 | A corrective maintenance facility is not organised and/or located to meet the agreed response times under normal circumstances. | 1 |
| 9.4.3 | L8 | Preventative maintenance record(s) not available and/or do not contain the required information. | 1 |
| 9.4.4 | L9 | Corrective maintenance record(s) not available and/or do not contain the required information. | 1 |
| 9.4.5 | L10 | Temporary disconnection record(s) not available and/or do not contain the required information. | 1 |

| | | | | | |
|-------------------------|--------------------------|--------------------|---|---------------------|-----------|
| Document no. | NSF 271 | Document issue no. | 2 | Document issue date | June 2021 |
| Document owner | Head of Approval Schemes | | | Last review date | June 2021 |
| Document classification | PUBLIC (RESTRICTED) | | | Page 10 of 10 | |