DOOR ACCESS CONTROL SYSTEM POLICY

1 PURPOSE

1.1 Electronic door access control systems are widely used in the National University of Singapore (NUS) to control access to buildings, offices and facilities. The use of door access control systems is to provide optimal physical security for the campus community and to protect the assets of NUS.

1.2 This policy seeks to:

a. provide security for NUS while enabling freedom of access to the NUS community;

b. facilitate management of all electronic door access control systems (DACS) installed in NUS, and

c. enhance security by providing procedures for the administration of all electronic door access control systems.

2 DEFINITIONS

2.1 For the purposes of this policy, the following definitions apply:

a. **NUS Door Access Control System (NUS DACS)** – Card-based system that is centrally linked to NUS IT network and used in conjunction with NUS access cards.

b. **Access Control Device** – Any mechanical or electronic, including but not limited to a key or an access card.

c. **Individual/Individuals** – Staff, Students or Visitors.

d. **NUS** – the National University of Singapore, comprising campuses in Kent Ridge, Bukit Timah, University Town and all other off-campus facilities.

e. **NUS access card** - Staff card, matriculation card, term card and temporary card.

f. **Site Administrator (SA)** – Staff appointed by Users to manage the DACS.

g. **Term Contractor** – Term Contractor supplying and maintaining DACS.
h. **Users** – Administrative Offices, Faculties, Research Institutes and Residential Occupants, Data Centres, Wire Centres and any other entities of NUS that employs DACS

i. **Exit Door** - *a door provided at the doorway of an exit for passage of people (according to fire code).*

### 3 SCOPE

3.1 This policy defines the DACS and procedures to govern the procurement, installation, administration and usage of the DACS in NUS.

3.2 This policy is applicable to all Users. Users shall keep existing system but shall comply when they need to upgrade the existing system.

### 4 NUS DOOR ACCESS CONTROL SYSTEM

4.1 NUS DACS is card-based and is used in conjunction with NUS access cards. NUS DACS is centrally linked and consists of an access control database, access control devices installed in the individual premises and management computer terminals. In order for authorised Individuals to access a facility, their card number has to be added to the authorised access list by the Site Administrator (SA). When accessing a facility, the holder of the authorised NUS access cards will have to tap on the card reader to access.

4.2 The following group shall be responsible for the following:

a. **Computer Centre (CC)** – to advise and manage all IT related issues relating to DACS

b. **Office of Campus Security (OCS)** – to develop and ensure compliance with DACS policy

c. **Office of Estate Development (OED)** – to coordinate procurement and installation of DACS for New and Addition & Alteration (A&A) projects managed by OED

d. **Office of Facilities Management (OFM)** – to facilitate a term maintenance contract for users to maintain DACS

e. **Office of Safety, Health and Environment (OSHE)** – to advise on safety standards and ensure compliance with statutory and university regulations

f. **Users (refer to definition)** – User shall be responsible for management and maintenance of their DACS
5 INSTALLATION OF DOOR ACCESS CONTROL SYSTEM

5.1 For consistency in security standards and efficiency in managing incidents during an emergency or crisis, Users shall install NUS DACS which is linked to the central door access database. Any deviations will need to be approved by Director, OCS. Users shall only install DACS that are in compliance. Users that have older DACS that are in non-compliance are required to ensure compliance whenever they undergo upgrading works to their DACS.

5.2 OFM will appoint and facilitate a term contract for the maintenance of NUS DACS. Users shall approach OFM to tap the term maintenance of DACS based on the contract rates. Users will liaise with OCS, CC, OFM and OSHE to coordinate the maintenance of DACS.

5.3 All DACS installed in NUS shall be registered with OCS and OSHE (for lab doors). It is the responsibility of Users to register with OCS whenever DACS is installed at their premises.

5.4 The funding for installation of the all DACS is to be provided by Users. Any DACS installed shall be the Assets of the Users and they shall manage and maintain the DACS (see Section 8.1).

5.5 Users shall coordinate with OCS/OSHE to ensure that installation of new DACS complies with policy and statutory fire and safety regulations.

Access Controls for Laboratories

5.6 To cater for the events involving unexpected power failure, malfunctioning of DACS, activation of fire alarm or other emergencies that require the evacuation of the occupants in the laboratories, the Exit Door serving any laboratories shall be designed to be “fail secure”.

5.7 A “fail secure” mechanism shall be installed that meets the following criteria:

a. Occupants shall continue to have unrestricted egress through the exit door
b. Only designated personnel (as determined by the lab/department) be allowed to enter the laboratory during such events mentioned in 5.6.
c. Provisions made for laboratory access for such designated personnel shall not rely on electric, electronic or other controls whose operation may be affected by such events mentioned in 5.6.
d. Provisions shall be made for emergency responders to bypass the door control system and enter the laboratory.
Access Controls for Data Centres/Wire Centres

5.8 DACS controlled doors of Data Centres / Wire Centres shall only allow access by authorized personnel.

6. **APPOINTMENT OF SITE ADMINISTRATOR**

6.1 Responsibility for the proper management of door access control systems rests with Users. The Dean/Director/Head shall appoint a Site Administrator (SA), who shall be a permanent staff member of NUS, to coordinate management of access list and all functional work areas relating to DACS. It is recommended that 2 SAs (Primary and Alternate) be appointed for DACS. This is to ensure that there is always a backup SA who can manage the access control system in the absence of the Primary SA. Dean/Director/Head shall also appoint a staff member of senior position to oversee the operation and conduct of SAs.

6.2 For NUS DACS, Users shall appoint up to 2 SAs and appointments should be made by the Dean/Director/Head. The SA/s appointed shall be permanent staff members. Individual user accounts will be given to each appointed SA and Users shall provide the following information to OCS before the issuance of user account to the SA:

   a. Department Name
   b. Name of Site Administrator
   c. Designation
   d. Staff Number
   e. Email Address
   f. Office Number
   g. Mobile Phone Number
   h. Doors to be controlled by the SA
   i. Appointment duration (if not permanent)

6.3 Users must inform OCS in writing if there is a change of SA. The new SA should be appointed and trained to manage the DACS when the existing SA is still available. Users shall ensure properly documented handover before the newly appointed SA takes over.

6.4 Users shall take disciplinary action against Individuals who deliberately disable the DACS.
7 SITE ADMINISTRATOR’S RESPONSIBILITIES

7.1 SAs are required to determine the DACS operational hours so as to regulate access to facilities under their charge. The DACS shall be activated on a 24-hour basis to ensure the effective usage of DACS. However, depending on the human traffic and level of activities at the facility during office hours, Users may activate DACS only after office hours. For such facilities, on special occasions (e.g. department retreat) when there is a need to adjust DACS operational hours (e.g. to lock doors during office hours), the SA shall be responsible for the locking/unlocking of DACS-controlled doors.

7.2 To facilitate the operation of DACS, SAs shall attend to queries regarding the DACS installed and liaise with the contracted maintenance service provider for all maintenance issues. In the event of a malfunction, SAs shall be responsible for activating the maintenance service provider, and shall take necessary measures to secure access to the facility before the arrival of the maintenance service provider.

7.3 SAs shall be responsible for granting access rights to authorised Individuals. Access to DACS controlled doors shall only be granted to Individuals who are authorised in the facility. Users shall have internal guidelines for their appointed SA/s to govern the granting of access. There should also be a system in place to communicate access changes to accommodate Individuals who are newly hired, enrolled, retired or have resigned. While users may have more stringent guidelines, the following are some considerations when granting access to Individuals:

a. Escort: If the need for access is infrequent, arises because of a special circumstance, or is short term, arrange for a responsible Individual to provide access.

b. Temporary Access: When access is needed on a temporary rather than permanent basis, a clear time frame for access should be established. If user has to issue temporary access device (e.g. temporary card or term card), there should be a proper handing and taking over procedure.

c. Hours of Work: If the facility is unlocked during an Individual’s normal working hours, and access is not needed at other times, User may not grant access to the Individual.

d. Access Area: User should only grant access to the least number of areas required for an Individual to perform his or her work. This may range from access to a single level in a single facility to multiple levels in multiple facilities.
7.4 If there is a need to grant temporary access rights, there should be documented approval before the granting of access. The documented approval should include the following information:

a. Name of person
b. NRIC/Foreign Identification number
c. Staff/Matriculation number
d. Designation
e. Email Address
f. Office Number and Mobile Phone Number
g. Reasons for accessing the premise
h. DACS controlled doors granted access
i. Approved access duration
j. Approval given by Dean/Director/Head or the appointed officer

7.5 SAs are also responsible for the timely removal of access rights when access authorization for an Individual expires. For facilities whereby the common doors are managed by OCS, the SA shall inform OCS when the Individuals are no longer authorised to access the facilities.

7.6 SAs shall ensure that activity records are not released to unauthorised persons.

8 MAINTENANCE OF DOOR ACCESS CONTROL SYSTEM

8.1 Users shall enter into a contract for regular maintenance for DACS installed. Amongst others, the maintenance service should cover emergency response by the maintenance service provider within an acceptable timeframe (should be less than 4 hours) to minimise downtime and inconvenience to facility occupants.

8.2 OFM will facilitate a term maintenance contract for NUS DACS. Users may procure the maintenance service based on the contract terms and conditions. The contract shall entail a periodical audit check by the maintenance vendors to ensure that the DACS and their supporting infrastructure are functioning as per design intent.

8.3 The funding for maintenance of all DACS is to be provided and borne by Users.

8.4 When the system malfunctions and the SA is not contactable, OFM or OCS shall have the right to activate the Supplier or any other vendors to respond and carry out the necessary repair and maintenance works. The costs incurred shall be borne by Users.
9  ACCESS DEVICE

9.1 Users may issue access devices (e.g. NUS access card, transponder, RFID tag etc) to facilitate usage of the installed DACS. There should also be a system in place to manage the issuance of access devices. When issuing access devices, Users shall ensure that they have the particulars of the receiver. The particulars should minimally include the name, identification number, contact number, address, email address, organization and designation.

9.2 To ensure the effectiveness of the DACS, it is the responsibility of holders of access devices to ensure that they report any loss of access devices to the issuer or system owner as soon as they are aware of the loss. The holder shall not share their access device at all times.

10  EMERGENCY & SECURITY

10.1 When there is a need to perform security patrol duties in DACS controlled premises, OCS will request the SA to grant the officer/s access. Access shall be granted to authorize OCS personnel and access device shall be provided to facilitate the access. For NUS DACS, the staff card of OCS personnel may be used to facilitate access.

10.2 OCS may request for relevant information (e.g. access records) of the DACS from Users for investigations and audit purposes. The Users shall provide OCS with the required information. For NUS DACS, OCS may also retrieve access records directly from the system during an investigation. OCS shall ensure that access records are not released to unauthorized persons.

10.3 For NUS DACS, OCS has the authority to override any existing command of the system in emergencies where there is an imminent threat to life and property (e.g. fire, crime in progress). Approval, however, must be given by at least one of the following personnel:
- Director, OCS
- Deputy Director, OCS
- Head Operations Division, OCS
- Director, OSHE
- Deputy Director, OSHE
- Head Emergency Management Division, OSHE

10.4 OCS/OFM/OSHE shall conduct selective audits to ensure compliance to policy. Users shall be required to facilitate the audits by providing relevant information and evidence. Based on the findings of the audits, OCS/OFM/OSHE may recommend measures to improve the management of the DACS. It is the responsibility of Users to ensure that the necessary corrective measures are implemented.
11 COMPLIANCE AND INDEMNITY

11.1 It is the responsibility of Users with DACS at their facilities to comply with the Door Access Control System Policy. Failure in compliance would be deemed as a violation of NUS security practices as promulgated in this policy.

11.2 Failure by Users to observe the provisions of this policy may result, whether directly or indirectly, in NUS being involved in claims and/or suffering damages, losses and/or expenses.

12 CHANGES TO POLICY

13.1 NUS reserve the right to amend this policy or implement additional policies when necessary. Users shall be informed of policy changes via email broadcast or timely updated documents. Users shall be solely responsible for staying informed about NUS’ policies, whenever such amendments have been made available to Users.

Professor Yong Kwet Yew
Vice President (Campus Infrastructure)

17 February 2014