NUS MANAGEMENT OF CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM POLICY

1. PURPOSE

1.1 This policy seeks to spell out the procedures on the management of the closed circuit television (CCTV) system within the University.

1.2 The CCTV system shall be managed in accordance with all relevant legislations, standards and University policies.

2. DEFINITIONS

2.1 For the purpose of this policy, the following definitions shall apply:-

a) Authorizing Officer - The Dean, Director or Head of the Administrative Offices, Faculties and Research Institutes or any entities in NUS which employs CCTV System in their facilities.

b) System Officer - An officer authorized by the Authorizing Officer to act on his behalf under this Policy.

c) System Operator - Person employed by the System Owner to monitor the CCTV system.

d) Unauthorized Personnel - Persons not authorized by the Authorizing Officer to have access to the CCTV.

e) Contractor - Contractor employed by the System Owner or User to install or maintain the CCTV system.

f) System Owner - Administrative Offices, Faculties and Research Institutes and any entities of NUS that owns the CCTV system.

g) User - Administrative Offices, Faculties and Research Institutes and any entities of NUS.

h) Emergency - Incidents that may lead to serious injury to people, or loss of life or serious damage to property.

3. CONCEPT OF OPERATIONS

3.1 The CCTV system is intended to provide an increased level of service, safety and security in the University environment. The CCTV system is part of an integrated security approach that includes physical security patrol, access control and alarms. The CCTV system may also be used for training purposes or managing access control and shall not be used to invade the privacy of any individual.
3.2 The system shall only be used for the following purposes:
   a) To prevent, deter and detect crime and also damages to property within the University,
   b) To assist in investigation and prosecution of incidents and offences,
   c) To facilitate emergency operations,
   d) To facilitate security deployments and operations.

4. SYSTEM DETAILS

4.1 The University has CCTVs installed in various locations and facilities. While majority of these CCTVs are linked to the Command Centre in OCS, some of the CCTVs are installed, monitored and supervised by the System Owner themselves.

5. DATA PROTECTION – PRIVACY

5.1 All data collected using this system, including images, will be managed in accordance with the NUS Data Policy relating to the control of information.

5.2 All persons involved in the operation of the system are obliged to exercise the upmost care to prevent improper disclosure of material.

6. INSTALLATION OF THE CCTV SYSTEM

6.1 To ensure that the University is in line with Ministry of Home Affairs guidelines in its usage of CCTV, OCS shall be consulted in writing if any User wishes to install CCTV in their buildings or facilities. Upon receipt of the request, OCS shall provide the necessary security and technical expertise for the User to consider.

6.2 All CCTV installed in the University shall have a minimum of 12 frames per second and also be continuously recorded.

6.3 All Users shall provide the necessary funding for the installation, management and maintenance of the CCTV system.

6.4 OCS is the staff authority for the installation of CCTV cameras in the University. Users are required to seek OCS’ approval before procurement and installation of the CCTV system. OCS will conduct a security review to assess the requirements and recommend the optimum number of cameras to be installed.
7. MANAGEMENT OF THE SYSTEM

7.1 The Authorizing Officer shall appoint a System Officer to be responsible for managing compliance with this Policy and inform Director OCS in writing.

7.2 The System Officer shall be responsible for the day-to-day management of the system and associated processes.

7.3 The System Officer shall ensure that CCTV recording in his system is archived for at least 30 days and shall also ensure that any CCTV in his system suffers less than 24 hours downtime.

7.4 The System Officer shall ensure an existing and valid maintenance service contract. Amongst others, the System Officer shall ensure the Contractor provides emergency response within less than 24 hours to minimize downtime. The funding for maintenance of the CCTV System is to be provided by the System Owner.

7.5 The System Officer shall maintain a CCTV System Register. Any fault, breakdown or system failure to the CCTV System detected shall be documented in the register. The System Officer is to ensure that proper documentation is maintained for future references.

8. PUBLIC INFORMATION

8.1 CCTV operations shall be overt in nature wherever possible. In cases where covert CCTV operations are warranted, approval shall be sought from Director OCS.

8.2 Whenever possible, signs that CCTV cameras are in operation shall be displayed at key positions and in proximity to the area under surveillance to inform staff, students and visitors. System Owner shall only install signs that have been pre-approved by OCS. A sample is attached in Annex A.

8.3 The policy shall be made available on the University staff portal.

9. BREACHES OF THE POLICY INCLUDING THOSE OF SECURITY

9.1 Any breach of the Policy shall be reported to the Authorizing Officer. The Authorizing Officer shall then direct an investigation and upon conclusion of the investigation consult Director OCS on the further course of action.

9.2 The University reserves the right to apply disciplinary measures for breaches, up to and including referring the breach to appropriate relevant authorities.
10. CONTROL AND OPERATION OF THE CAMERAS

10.1 The CCTV shall only be operated by person(s) under the employment of the System Owner and approved by the System Officer.

10.2 The System Operator shall only be allowed to monitor and conduct virtual patrol with the CCTV system. The System Operator and System Officer shall ensure that the CCTV is capturing the recording as in accordance to Para 3 and shall not abuse or use the CCTV for any mischief.

10.3 The System Officer may direct a replay and review of the CCTV recordings. To prevent mishandling of all recorded material, all recorded footage shall be controlled by the System Officer.

11. ACCESS TO CCTV

11.1 The System Officer shall ensure access to the system is restricted to the System Operators and persons authorized by the Authorizing Officer. Any request to view or access the CCTV System shall only be acceded with the approval of the Authorizing Officer. Any approval shall be recorded in the register.

11.2 In cases of Emergency, System Operators or System Officers shall at their discretion allow rescue personnel or security responders to have access of the CCTV System.

11.3 With the approval of Director OCS, OCS staff may request CCTV footages from System Owners for investigations and audit purposes. The System Owner shall provide OCS with the required footage within 24 hours of the request. This request shall be made in writing by Director OCS to the System Owner.

12. RECORDED MATERIAL

12.1 All recorded material shall not be sold or used for commercial purposes.

12.2 Snapshots of the CCTV System shall only be taken by the System Officer. He shall not hand this over to any persons without prior approval from the Authorizing Officer in consultation with Director OCS.

12.3 A written record of the request including details of the requesting officer, time and date of the request and the reasons shall be made and documented in the register. The System Officer shall ensure that the snapshot is properly labeled with the date, time and location of the recording before handing it over to the requestor. A sample is attached in Annex B.

12.4 The requestor shall be made to sign that he/she shall only use the snapshot for official purposes and use it in a responsible manner and shall not distribute it without prior approval from the Authorizing Officer and Director OCS. A sample is attached in Annex C.
13. COMPLIANCE AND INDEMNITY

13.1 It is the responsibility of System Owners with CCTV at their facilities to comply with the NUS Policy for Management of Closed Circuit Television System. Failure in compliance would be deemed as a violation of NUS security practices as promulgated in this policy.

13.2 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.

14. CHANGES TO POLICY

14.1 NUS reserves the right to review 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’ polices, whenever such amendments have been made available to Users.

Prof Tan Chorh Chuan
President

13 Apr 2011
WARNING

AREA UNDER CAMERA SURVEILLANCE

Office of Campus Security
Hotline: 6874 1616

You are being watched!
This CD contains footage of:

1)  
2)  
3)  
4)  

Location: E1, 2nd Floor (sample)
Date and time of footage: 31 Feb 2010, 1500 - 1600hrs (sample)
Source of footage: School of Computer (sample)
Signed and Verified by: [System Officer], date
CCTV FOOTAGE AT XXXX ON XXXX FROM XXXXHRS TO XXXXHRS.

Dear Sir/Mdm,

1. To facilitate your preparation of an XXXX, we shall be releasing certain relevant confidential information and CCTV footages. In consideration of such release, you hereby acknowledge and agree that the release of the Confidential Information is subject to and upon the following terms and conditions:

1.1 You hereby agree to hold and keep in strictest confidence any and all Confidential Information.

1.2 You undertake that the Confidential Information shall be used only for the purpose of investigation and you shall take all steps and measures to minimize the risk of disclosure of the Confidential Information.

1.3 You shall ensure that the Confidential Information will not be copied or reproduced in any form whatsoever by you or any third parties save as may be necessary for the purposes contemplated in Clause 1.2.

1.4 You shall ensure the security and control of any Confidential Information which is in documentary or other tangible or intangible form by physically restricting the location and use of such Confidential Information to areas of restricted access and by storing such Confidential Information in a manner which does not permit unauthorized access.
1.5 You shall promptly destroy such Confidential Information or if they are in paper form shred such Confidential Information using a shredding machine upon completion of your investigation.

1.6 You shall not publish any of the Confidential Information or make any references, statements, announcements or denial or confirmation in any medium concerning the Confidential Information without the express written permission of NUS, which permission may be granted or withheld in NUS’ sole discretion.

2. Whilst every effort and care have been made to ensure that the Confidential Information provided herein is up to date and accurate, NUS does not hold any responsibility and will not be made liable for any loss or damage of any kind whatsoever arising as a result of any inaccuracies or omissions in the Confidential Information.

3. Should you require clarifications with regards to security of these recordings, feel free to contact Mr. XXXX, Manager, (Department) at xxxx@nus.edu.sg.

4. Please indicate your acceptance of the above terms and conditions by signing on and returning a copy of this Agreement.

Sincerely,

Name of Manager
Department

I hereby agree to the above terms and conditions.

Name/Designation/Department

Xx Kent Ridge Road, Singapore xxxxxx Tel: (65) xxxxxxx Fax: xxxxxxxx
Website: http://www.nus.edu.sg