Appendix X

Contingency Plan for Different Threats in Different Locations (including Computer Laboratories) - Information Technology Services Office (ITSO)

1. IN SERVER ROOM

1.1 In case of Fire/Smoke/Fire Suppression System Alert

(a) Evacuate all personnel inside immediately. Fire suppression system installed in the room would trigger an alarm and release gas (e.g., FM200) for fire suppression.
(b) Call Security Control Room at **3190 6610** or **999**.
(c) Follow Emergency Procedures of FMO for fire.
(d) Re-enter the site when the room is safe.
(e) Evaluate all equipment, cable and fiber in the vicinity of the fire for potential damage.
(f) Test other data cables for damage.
(g) Evaluate and test all electronic equipment that have been exposed to water.
(h) Assess all equipment to assure adequate ventilation remains.

1.2 In case of Water Leakage

(a) Call Security Control Room at **3190 6610**.
(b) Take away electronic equipment possibly affected by the leakage.
(c) Re-enter the site when the room is cleanup.
(d) Evaluate all equipment, cable and fiber in the vicinity of the water leakage for potential damage.
(e) Test other data cables for damage.
(f) Evaluate and test all electronic equipment that have been exposed to water or other agents.
(g) Assess all equipment to assure adequate ventilation remains.

1.3 In case of Power Outages

(a) Call Security Control Room at **3190 6610** for maintenance.
(b) Re-enter the site when power is resumed.
(c) Evaluate and test all electronic equipment.

1.4 In case of Air Conditioning Outages

(a) Call Security Control Room at **3190 6610** for maintenance and arrange fan for ventilation.
(b) Evaluate and test all electronic equipment when air conditioning resumes.

1.5 In case of Network Outages

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Helpdesk staff help to communicate with users and advise them the progress of repair.
(c) Evaluate and test all electronic equipment when network connection resumes.

1.6 In case of Denial of Service Attack

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Isolate the server from the Campus Network if possible.
(c) Try to locate the attacker from the intrusion prevention system and block the IP address.

2. IN NETWORK SWITCH ROOM

2.1 In case of Fire/Smoke

(a) Evacuate all personnel inside immediately.
(b) Call Security Control Room at **3190 6610** or **999**.
(c) Follow Emergency Procedures of FMO for fire.
(d) Re-enter the site when the room is safe.
(e) Evaluate all equipment and cable in the vicinity of the fire for potential damage.
(f) Test other data cables for damage.
(g) Evaluate and test all electronic equipment that have been exposed to water.
(h) Assess all equipment to assure adequate ventilation remains.

2.2 In case of Water Leakage

(a) Call Security Control Room at **3190 6610**.
(b) Take away electronic equipment possibly affected by the leakage.
(c) Re-enter the site when the room is cleanup.
(d) Evaluate all equipment and cable in the vicinity of the water leakage for potential damage.
(e) Test other data cables for damage.
(f) Evaluate and test all electronic equipment that have been exposed to water or other agents.
(g) Assess all equipment to assure adequate ventilation remains.

2.3 In case of Power Outages

(a) Call Security Control Room at **3190 6610** for maintenance.
(b) Re-enter the site when power is resumed.
(c) Evaluate and test all electronic equipment.

2.4 In case of Air Conditioning Outages

(a) Call Security Control Room at **3190 6610** for maintenance and arrange fan for ventilation.
(b) Evaluate and test all electronic equipment when air conditioning resumes.

2.5 In case of Network Outages

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Helpdesk staff help to communicate with users and advise them the progress of repair.
(c) Evaluate and test all electronic equipment when network connection resumes.

2.6 In case of Denial of Service Attack

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Try to locate the attacker from the intrusion prevention system and block the IP address.

3. IN OFFICE

3.1 In case of Fire/Smoke

(a) Evacuate all personnel inside immediately.
(b) Call Security Control Room at **3190 6610** or **999**.
(c) Follow Emergency Procedures of FMO for fire.
(d) Re-enter the site when the room is safe.
(e) Evaluate all equipment and cable in the vicinity of the fire for potential damage.
(f) Test other data cables for damage.
(g) Evaluate and test all electronic equipment that have been exposed to water.

3.2 In case of Water Leakage

(a) Call Security Control Room at **3190 6610**.
(b) Take away electronic equipment possibly affected by the leakage.
(c) Re-enter the site when the room is cleanup.
(d) Evaluate all equipment and cable in the vicinity of the water leakage for potential damage.
(e) Test other data cables for damage.
(f) Evaluate and test all electronic equipment that have been exposed to water or other agents.

3.3 In case of Power Outages

(a) Call Security Control Room at **3190 6610 f**or maintenance.
(b) Re-enter the site when power is resumed.
(c) Evaluate and test all electronic equipment.

3.4 In case of Air Conditioning Outages

(a) Call Security Control Room at **3190 6610** for maintenance and arrange fan for ventilation.
(b) Evaluate and test all electronic equipment when air conditioning resumes.

3.5 In case of Network Outages

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Helpdesk staff help to communicate with users and advise them the progress of repair.
(c) Evaluate and test all electronic equipment when network connection resumes.

3.6 In case of Denial of Service Attack

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Isolate the computer from Campus Network.
(c) Try to locate the attacker from the intrusion prevention system and block the IP address.

3.7 In case of Epidemics

(a) Arrange equipment loan if needed.

4. IN TEACHING SITES

4.1 In case of Fire/Smoke

(a) Evacuate all personnel inside immediately.
(b) Call Security Control Room at **3190 6610** or **999**.
(c) Follow Emergency Procedures of FMO for fire.
(d) Help teacher to arrange another classroom to continue the class activities or use web conferencing.
(e) Re-enter the site when the room is safe.
(f) Evaluate all equipment and cable in the vicinity of the fire for potential damage.
(g) Test other data and audio-visual cables in the teaching site for damage.
(h) Evaluate and test all electronic equipment that have been exposed to water.

4.2 In case of Water Leakage

(a) Call Security Control Room at **3190 6610**.
(b) Take away electronic equipment possibly affected by the leakage.
(c) Help teacher to arrange another classroom to continue the class activities or use web conferencing.
(d) Re-enter the site when the room is cleanup.
(e) Evaluate all equipment and cable in the vicinity of the water leakage for potential damage.
(f) Test other data and audio-visual cables in the teaching site for damage.
(g) Evaluate and test all electronic equipment that have been exposed to water or other agents.

4.3 In case of Power Outages

(a) Call Security Control Room at **3190 6610** for maintenance.
(b) Help teacher to arrange another classroom to continue the class activities or use web conferencing.
(c) Re-enter the site when power is resumed.
(d) Evaluate and test all electronic equipment.

4.4 In case of Air Conditioning Outages

(a) Call Security Control Room at **3190 6610** for maintenance and arrange fan for ventilation.
(b) Help teacher to arrange another classroom to continue the class activities or use web conferencing.
(c) Evaluate and test all electronic equipment when air conditioning resumes.

4.5 In case of Network Outages

(a) Call IT Helpdesk at **3190 6640** for support immediately.

(b) Help teacher to arrange another classroom to continue the class activities or use web conferencing.
(c) Evaluate and test all electronic equipment when network connection resumes.

4.6 In case of Denial of Service Attack

(a) Call IT Helpdesk at **3190 6640** for support immediately.
(b) Isolate the computer from Campus Network.
(c) Reboot the computer.
(d) If the attack persist, help teacher to arrange another classroom to continue the class activities or use web conferencing if needed.
(e) Replace the computer.
(f) Try to locate the attacker from the intrusion prevention system and block the IP address.

4.7 In case of Epidemics

(a) Switch to online teaching mode using web conferencing.

5. ACCIDENT/INCIDENT REPORTING

(a) Any incident occurring in office/teaching site during school hours must be reported immediately to School or IT Helpdesk at Tel. 3190 6640.
(b) After school hours, the incident should be reported to Security Control Room at Tel. 3190 6610 (emergency response)
(c) All incidents must be reported to Security Control Room and School Executive Officer within 24 hours or the following working day.
(d) Be prepared to provide the Security Guard with sufficient details for an incident report.