Title:
Sample ACCESS CARD/IDENTIFICATION CONTROL POLICY

1. PURPOSE

The purpose of this policy is to outline a process for controlling Access Card/Identification (Access Card/ID) at COM X Technologies, Inc. (COM X), and to ensure the protection of COM X personnel and property through the electronic control of access to doors, rooms and other secure areas/spaces at the COM X in XX.

2. SCOPE

2.1 This policy applies to all COM X employees, temporary staff members, consultants, and contractors/vendors who work at COM X in XX

2.2 This policy applies to all guests and visitors that are issued or that use an Access Card/ID at COM X in XX.

3. DEFINITIONS

3.1 Access Card/ID

A COM X Access Card/ID is an electronically coded card which allows employees access to the facility and other restricted areas within the facility, as applicable. The Access Card/ID has a unique number on one side of the card which is assigned to one employee.

3.2 Access Card/ID Control Officer

The Director of Security (DoS) or designee will be the Access Card/ID Control Officer and is responsible for the issuance and control of all Access Card/IDs, and for the control and maintenance of card readers.

3.3 Employee Identification

Incorporated on the Access Card/ID is Employee Identification information (ID), which includes a photo of the employee, the employee's date ofhire and the employee's ID (employee) number.

3.4 Visitor/Vendor/Contractor Access Card/ID

A COM X VisitorNendor/Contractor badge is a distinct badge that identifies the wearer as a visitor to the facility. This badge may include a photo of the visitor, the visitors name or the COM X logo, and a RED or GREEN COM X shield.

4. RESPONSIBILITIES

4.1 Initiator

The Initiator is responsible for updating/maintaining this Policy when the procedure changes.

4.2 User

4.2.1 The Users are COM X employees, temporary staff members, consultants, contractors/vendors and visitors or guests who enter COM X Access Card/ID Controlled space. The users are responsible for reading, understanding and following this policy.

4.2.2 All Users will be required to acknowledge receipt of, and understanding of all applicable COM X policies and procedures. They will be required to sign the policy control document accepting responsibility for the information contained therein.

'f< 5. POLICY

5.1 Visitors/Vendors and Contractors

5.1.1 All visitor badges must be returned at the end of each day.

5.1.2 Access Card/ID that provides access to card readers and therefore COM X secure space, will only be issued to visitors, vendors and contractors of COM X as outlined in the COM X Security Access Card/ID Procedures (**-0005-SEC V-1.0)

5.2 Personnel Authorized to Issue Cards

5.2.1 Issuance of Access Card/ID(s) maybe authorized by those indicated in Appendix 1, *COM X Authorized Issuers List.*

5.2.2 Designated COM X personnel outlined in Appendix 1 retain the right to access all Hard Key and Access Card/ID controlled areas as warranted for COM X safety or investigative purposes.

5.3 Duplication of Access Card/IDs

No Access Card/ID(s) will be duplicated. The unauthorized duplication ofCOM X Access Card/ID so adversely affects the security of persons and property that violations of this rule are considered serious and grounds for discipline up to and including termination.

5.4 Numbering System for Access Card/IDs

An identifying number is stamped on the back of each Access Card/ID. The serial number for each Access Card/ID will be unique to the individual Access Card/ID.

5.5 Lost, Stolen or Damaged Access Card/ID

5.5.1 Reference COM X Security Access Card/ID Procedure (**- 0005-000 V-1.0)

5.5.2 A new Access Card!ID will not be issued to anyone who was previously assigned an Access Card/ID unless a *COM X Security Incident Report* is completed by the reporting individual and is on file with the DoS. *Do not wait to report an incident even if you are unable to complete the forms immediately.*

5.6 Termination, Retirement Separation from the COM X

Upon termination of employment from COM X the Access Card/ID will be surrendered immediately. However, failure to return Access Card/ID badges will in no way halt or delay the completion of the separation process. Reference COM X Security Access Card/ID Procedure (**-0005-SEC V-1.0)

5.7 Repair or changes to locking devices or access system hardware

5.7.1 No COM X area, space, cabinet maybe secured except by a locking device authorized for that area and with an operating code compatible with the COM X Access Card/ID system. The DoS will be provided with and will maintain keys to all COM X owned areas, spaces, cabinets, etc. Exceptions include personal padlocks for unassigned lockers in all the locker/restroom areas.

5.7.2 Any person causing an unauthorized repair to a COM X lock or door hardware is in violation of COM X policy.

5.7.3 Reference: COM X Security Access Card/ID Procedure (**- 0005-000 V-1.0).

5.8 Storage of Access Card/ID(s)

All Access Card/ID blanks ready for programming/issue will be stored by the DoS in a locked controlled cabinet/space until printed and issued.

5.9 High Security Areas:

5.9.1 SERVER ROOM ACCESS

Access to the Server Room (1008) will be issued only to authorized personnel by the Vice President of Information Technology or designee or the DoS in their absence.

5.9.2 DOCUMENT CONTROL ROOM ACCESS

Access to the Document Control Room (1011) will be issued only to authorized personnel of the Chief Scientific Officer. Reference: Document Control Room (SOP 00)

5.9.3 LAB SPACE ACCESS

Lab Space for all areas will be controlled by Hard Key, Access Card/ID and Number Pad and will require at minimum dual authentication for access.

5.10 Access Card/ID Issuance to Outside Contractors

Repairs of COM X facilities which require a contractor to be issued an Access Card/ID to any area must be approved by the DoS or designee. Reference: Access Card/ID Procedures (**0005-000 V-1.0).

6. RECORDS

NOTE: The DoS shall maintain a record of all Access Card/ID that are issued and retrieved. Hard copies of these records will be stored in a locked file maintained by the DoS. Electronic copies will be stored in R: / SecurityDocs/Access Card/ID folder.

7. REFERENCES

7.1 COM X *Security Access Card/ID Procedure (**- 0005-000 V-1.0)*

7.2 *Document Control Room (SOP 00)*

8. APPENDICES

Appendix 1, *COM X Security Authorized Issuers List*

9. CHANGE(S) FROM PREVIOUS VERSION

Version Number	Section/Step Number	Changes/Reason
2.0	5.7.	Revised-title language updated
2.0	5.9.2	Revised-Removed Designee