



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 1 of 14

1.0 PURPOSE

- 1.1 The purpose of this facility access control policy is to describe the processes in place to aid in providing a safe and secure environment for Cell Signaling Technologies ("CST").
 - 1.1.1 It will establish the responsibility, eligibility, and approval process for members of the CST Community to be granted access to CST property through a variety of means, including access cards and mechanical keys.
- 1.2 This policy and supporting guidelines set out specific responsibilities, conditions and practices that are designed to address access requirements in a manner that minimizes risks to personal safety and maximizes physical asset protection.

2.0 SCOPE

- 2.1 This policy applies specifically to the CST US facilities located at 3 Trask Lane, Danvers and 32 Tozer Road, Beverly.
- 2.2 This policy applies to all members of the CST community, including visitors, contractors, vendors, temporary and approved external users, having authorized access to any CST owned or leased space.
- 2.3 This policy will govern all methods of physical access control including but not limited to mechanical key systems, specialized security access systems, card access control systems, and any system designed to control an area or facility access point.
- 2.4 This policy and supporting guidelines will be periodically reviewed and updated to reflect active security requirements consistent with employee safety and asset protection. The modular nature of this policy enables more frequent updates to address emerging threats and new security measures. The provided security criteria will assist the Chief Security Officer with designing and implementing a uniform level of security protection while providing the autonomy to institute more stringent security measures and controls based on CST's business needs.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 2 of 14

3.0 DEFINITIONS

- 3.1 Access Control: regulates who can access physical space or digital information
- 3.2 Access Card: physical access card granting access to property and spaces
- 3.3 Company: Cell Signaling Technology
- 3.4 Contractors: see Vendor
- 3.5 Contract Employee: an independent contractor or 1099 employee. Someone who provides a service for a fee.
- 3.6 Essential Employee: an individual necessary to maintain business continuity
- 3.7 Metal Keys: mechanical keys grant location access based on role and responsibility.
- 3.8 Piggyback: when a person tags (follows) along with another person who is authorized to access a property, without presenting access credentials
- 3.9 Restricted: property or spaces that retain restricted access
- 3.10 Security Personnel: any/all personnel involved with security administration, procedures, and processes
- 3.11 Surveillance: monitoring of behavior, activity and information
- 3.12 Temporary Personnel: employee who is hired for a limited time typically less than nine months
- 3.13 Vendor: contract employees, outside consultants, subcontractors, suppliers, or other outsourced people who provide services (or products).
- 3.14 Visitor: a person visiting a place or person, socially or otherwise
- 3.15 Visitor Log: paper visitor log that provides an audit trail of visitors
- 3.16 Volunteer: an individual who freely gives their time and labor.

4.0 ROLES AND RESPONSIBILITIES

- 4.1 The safety and security of the physical space and assets are a shared responsibility of all members of the CST Community.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 3 of 14

- 4.1.1 To meet this obligation, the Facilities Department has established this access control policy to address the hardware, software, operations, and administration of the access control system.
- 4.1.2 Only Facilities Department authorized access control systems shall be used at CST facilities.
- 4.2 Roles of individuals involved with the procedure:
 - 4.2.1 Chief Security Officer (CSO): The Facilities Director shall be designated as the CSO for all CST owned property. The role of the CSO is the security of physical assets, employees, and information in both physical and digital form.
 - 4.2.2 Assistant Security Officer (ASO): Facilities Supervisor(s) shall be designated as ASO's. The role of the ASO is to assist in the planning and execution of security measures and procedures for the organization.
 - 4.2.3 Information Officer: The Information Officer shall be filled by a member(s) of CST's Information Technology (IT) department. The role of the Information Officer shall be to follow the direction of the CSO while assisting with the execution of security measures and procedures for the Organization
- 4.3 Responsibilities of Individuals involved with the procedure:
 - 4.3.1 The Facilities Department or their designee shall:
 - 4.3.1.1 Ensure that restricted areas are protected by appropriate entry and controls for authorized personnel
 - 4.3.1.2 Control and validate a staff member's access to facilities with the use of mechanical keys, or electronic key cards.
 - 4.3.1.3 Establish visitor controls including visitor sign-in logs and wearing of visitor badges for both entry and exit of CST property



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 4 of 14

- 4.3.1.4 Periodic review of the list of individuals with physical access to facilities containing sensitive information, at the discretion of the CSO.
- 4.3.1.5 Maintain a complete inventory of critical assets with the Facilities Department and/or Information Technologies.
- 4.3.1.6 Card access records and visitor logs for facilities are available for periodic review based upon the criticality of the information being protected and security necessity
- 4.3.2 The Information Technology Department or their designee shall:
 - 4.3.2.1 Create access cards for new employees
 - 4.3.2.2 Assign employee access privileges
 - 4.3.2.3 Create replacement cards for lost or stolen access cards
 - 4.3.2.4 Disable or destroy cards as required
 - 4.3.2.5 Ensure IT assets are inventoried and physically protected

5.0 GUIDELINES

5.1 GENERAL

- 5.1.1 Physical access to all CST owned or leased properties shall be physically protected relative to the criticality or importance of the function or purpose within that facility.
- 5.1.2 Requests for access shall come from the applicable manager in the area where the process/data/system resides.
- 5.1.3 Access to facilities will be granted only to personnel whose job responsibilities require access.
- 5.1.4 Electronic access control systems shall be used to manage access to restricted spaces and facilities.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 5 of 14

5.1.5 The process for granting new employee and replacement access cards resides with the IT Department.

5.1.6 The Facilities Department shall be responsible to create and manage access rights.

5.1.6.1 They shall regularly review card and/or key access rights and remove access for individuals that no longer require access or persons who leave the Company.

5.1.6.2 Access rights shall be based on an employee's (staff, visitor, contractor, etc.) role or function in the organization.

5.2 CONTROL PROCEDURES

5.2.1 To effectively manage Access Control to Cell Signaling Technology and to protect the safety of all employees and visitors, the following procedures shall be followed:

5.2.1.1 All personnel shall be issued an access card upon hire.

5.2.1.2 It is not permitted to share access cards.

5.2.1.3 It is not permitted to issue more than one access card per employee.

5.2.1.4 It is highly recommended not to Piggyback into a building or secured area. Do not allow anyone you do not know to enter CST property

5.2.2 The Access Control System shall contain programming functionality to limit access and manage schedules.

5.2.3 The issued access ID card shall contain sufficient information to identify the individual.

5.2.3.1 First name and portrait photograph only.

5.2.3.2 Photograph and first name shall appear on the front side of the badge. Note: the front side of an access badge will not contain any alphanumeric printed information.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 6 of 14

5.2.3.3 No additional identification information shall be displayed on the access card i.e. Last name, company name, logo or company address.

5.2.4 Facilities and IT shall be notified of all separations or terminations of employees, contract employees, temporary employees and contractors allowing access card deactivation.

5.2.4.1 The employee/temporary/contractor employee's manager/HR is responsible for collecting the access card upon separation and returning it to Facilities or IT.

5.3 ACCESS CARD ISSUANCE:

5.3.1 All requests to produce a new access card or modification of an existing card shall be provided by:

5.3.1.1 Human Resources for new employees,

5.3.1.2 Employees Manager for transferred employees or for current employees requiring access modification

5.3.1.3 Relationship Manager for vendor/contractors

5.3.2 New employee access requests shall be in the form of a service request.

5.3.2.1 The service request shall be sent to IT.

5.3.2.1.1 IT: servicedesk@cellsignal.net

5.3.3 It is the responsibility of the IT Department to enter the new employee data into the access control system following the guidelines of the system and this policy.

5.3.3.1 The IT Department has the authority to issue employee access levels to new employees

5.3.3.2 All other access privileges, restricted area, specialize access levels, etc., shall be provided by the CSO.

5.4 KEY ISSUANCE



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 7 of 14

5.4.1 Facilities Management manages key issuance and shall maintain a listing of issued keys and share this listing with HR on an as needed basis.

5.4.1.1 See Key Loan Request Form, attached

5.4.2 Procedures for issuing keys should emulate that of access control cards, in that a request for keys should be completed by the employee's manager.

5.4.3 The issuance of physical keys should be limited and highly scrutinized, as the management of lost, stolen, or unreturned keys is a difficult process.

5.4.4 Keys that control the perimeter of any building shall not be issued unless required specifically for an individual's job function, or as approved by the Director of their department.

5.4.4.1 Issuance of such keys will be to departments only –not to an individual, unless approved by the Chief Security Officer.

5.4.5 Temporary employees, contract employees and/or volunteers shall not be issued mechanical keys on a permanent basis.

5.4.5.1 Should a mechanical key use be required to fulfill a job function, keys shall be managed within the requesting department and signed in/out to the temporary employee on an as-needed basis.

5.5 TEMPORARY PERSONNEL

5.5.1 In some scenarios, temporary personnel, contractors, vendors or volunteers (referred to as temporary employees) may be required to support CST operations.

5.5.2 Temporary personnel that frequent the Company or are assigned to an Essential Services role shall be eligible to receive access cards.

5.5.3 The manager responsible for the relationship shall authorize the required access.

5.5.4 All temporary cards shall have an expiration date consistent with the temporary employee contract term.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 8 of 14

5.5.4.1 In all separations or terminations, Security shall be notified.

5.5.5 The length of expiry on any temporary card may be extended upon the relationship manager's written approval (ie: e-mail).

5.6 VISITOR AND GUEST ACCESS

5.6.1 The following policy and procedure apply to the identification and authorization of visitors and guests to CST Properties:

5.6.1.1 Any CST facility that allows access to visitors shall track visitor access with a sign-in/out log

5.6.1.1.1 Visitor log will be located at the reception desk.

5.6.1.2 The visitor log shall be used to maintain a physical audit trail of visitor activity to the facility. Visitors must sign in and sign out during each visit.

5.6.1.3 The visitor log shall document the date and time of arrival and departure, visitor's name, the firm represented, and the on-site personnel authorizing physical site access.

5.6.1.3.1 The visitor log is maintained by Human Resources through the receptionist at each site.

5.6.1.4 The visitor log shall be retained for a minimum of three months, unless otherwise designated by rule, regulation, statute, or CST audit control

5.6.1.5 Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel

5.6.1.6 Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration

5.6.1.7 Visitors shall be authorized, by a CST employee, prior to entering the property and always be escorted within the facility.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 9 of 14

5.6.1.8 It is the responsibility of the CST authorized individual to coordinate escort compliance.

5.6.1.8.1 Areas where sensitive information is processed or maintained require an escort.

5.6.1.8.2 Visitor/guest access to secure areas shall be coordinated in advance by the onsite CST representative.

5.6.1.9 Visitors must be escorted in card access-controlled areas

5.7 RESIGNATIONS AND TERMINATIONS

5.7.1 Facilities and IT shall be notified in writing, where possible, of a termination or separation slated to take place. As this is a sensitive area for HR, Management and the Employee, caution should be used in the handling and timing of the deactivation of terminated employee's access card.

5.7.2 Once a termination has taken place, the access card and mechanical key(s) shall be collected by HR..

5.7.2.1 The access card shall be returned to Facilities, and all access associated with the ID card removed, and the card destroyed.

5.7.2.2 Mechanical keys will be returned to inventory and the key loan sheet shall be updated.

5.7.3 If the terminated employee did not have his/her ID card or key(s) on their person, HR shall ask that the access card and key(s) be mailed back to Security. Security shall be notified and will remove all access associated with the card and return key(s) to inventory.

5.7.4 If HR was unable to retrieve the card or key(s) for any other reason, Security shall be immediately notified, and the above steps shall be followed.



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 10 of 14

5.7.5 Terminated employees should not be allowed back into the workspace following the termination.

5.8 LOST OR STOLEN ACCESS CARDS

5.8.1 Access access cards act as keys and should be treated as such if lost or stolen.

5.8.2 Lost or Stolen badges must be reported to Security immediately.

5.8.3 Lost or stolen badges shall have access removed from the card immediately upon notification.

5.8.4 There shall not be any fee associated with replacing lost or stolen badge/access cards or mechanical keys.

5.8.5 If an access card that was lost is later found, it should be turned into security to remove all access and be destroyed.

5.9 RESTRICTED AREA ACCESS

5.9.1 The following policy and procedure apply to restricted area access:

5.9.1.1 All areas containing sensitive information, equipment, processes and/or present a safety risk shall be physically restricted

5.9.1.2 Confidential IT areas such as data centers, computer rooms, network closets, asset inventory, and similar areas containing IT resources shall be restricted based upon functional business need

5.9.1.3 Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 11 of 14

5.10 AUDIT CONTROLS AND MANAGEMENT

5.10.1 Evidence of practice should be in place for this operational policy as part of normal CST operations. Examples of acceptable controls and procedures include:

5.10.1.1 Visitor logs

5.10.1.2 Access control procedures and processes

5.10.1.3 Operational key-card access and premise control systems

5.10.1.4 Operational video surveillance systems

5.11 ENFORCEMENT

5.11.1 Staff members found in policy violation may be subject to disciplinary action in line with HR Policy, up to and including termination.

5.12 EXCEPTIONS

5.12.1 Any individual, group, or department who wishes to be granted an exception to this policy, must provide the following information relevant to the request:

5.12.1.1 Explanation on why this exemption is being requested

5.12.1.2 Details regarding the mitigating factors and compensation controls that will be used to offset the risk

5.12.1.3 Length of time for which the exemption is being requested (i.e. day, week, month, etc)

5.12.1.4 Requestor's name, email address, group or department and if more than one individual a list of personnel included in the exception

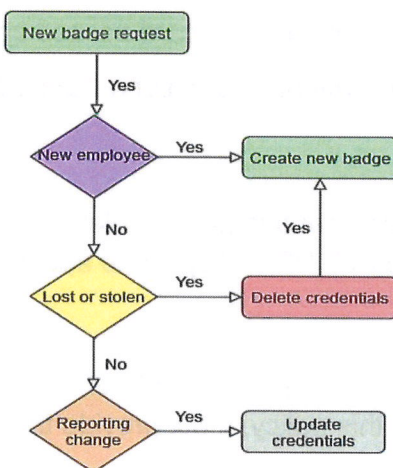
5.12.2 All exceptions are subject to approval by the Chief Security Officer.

**Title:** 00723-SOP Facility Access Control, Rev 01**Owning Department:** Facilities**Page 12 of 14**

6.0 PROCESS FLOW

6.1 New badge request diagram

New badge request diagram



Originator: Peter Muto
Rev: v.1
Date: 12Mar2021



Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 13 of 14

7.0 REFERENCES:

7.1 Facilities Asset List: FM:Interact asset listing (*at current revision*)

7.2 Visitor Log: Log-120-Visitor-A (www.bookfactory.com)


Title: 00723-SOP Facility Access Control, Rev 01

Owning Department: Facilities

Page 14 of 14
8.0 APPENDIX AND ATTACHMENTS (if applicable)

8.1 "Key Loan Request Form"

Key Loan Request Form	
Revision	v.1
Origination date	8Mar2021

Key Loan Request Detail Section	
Requestor printed name	
Key Number	
Hook Number	
Description of Locked Items	
Location of Locked Items	

Key Loan Request Signoff Section	
Request Date	
Print name	
Requestor signature	

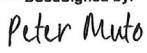
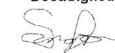
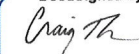

Key Loan Request Return Signoff Section	
Return Date	
Print name	
Signature	

CONFIDENTIAL AND PROPRIETARY INFORMATION OF CELL SIGNALING TECHNOLOGY, INC. This document and the information contained in it are the sole and exclusive property of Cell Signaling Technology, Inc. No right is hereby granted to use, disclose, reproduce or alter this document or any information contained therein, in whole or in part, for any purpose, unless expressly authorized in a signed writing by Cell Signaling Technology, Inc. These restrictions do not limit the right to use information legally obtained from a third party source. This document is issued as a REFERENCE COPY and is not revision controlled, unless otherwise indicated by Cell Signaling Technology, Inc. internal procedures.

**Title:** 00723-SOP Facility Access Control, Rev 01**Owning Department:** Facilities**Page 1 of 1****00723-SOP REVISION HISTORY**

01: New Document

SIGNATURE APPROVALS

Peter Muto ORIGINATOR	DocuSigned by:  AB807E67DCEB4E8... SIGNATURE	July 29, 2021 17:16 EDT DATE
Sang Park IT OPERATIONS	DocuSigned by:  C5B8B85A5C6E9DE... SIGNATURE	July 29, 2021 19:42 EDT DATE
Craig Thompson SVP GLOBAL OPERATIONS	DocuSigned by:  8E1E347D2E8D94E1... SIGNATURE	July 29, 2021 11:21 EDT DATE
Brian McDonough QUALITY	DocuSigned by:  61DC18C1D3304DB... SIGNATURE	July 30, 2021 07:22 EDT DATE

CONFIDENTIAL AND PROPRIETARY INFORMATION OF CELL SIGNALING TECHNOLOGY, INC. This document and the information contained in it are the sole and exclusive property of Cell Signaling Technology, Inc. No right is hereby granted to use, disclose, reproduce or alter this document or any information contained therein, in whole or in part, for any purpose, unless expressly authorized in a signed writing by Cell Signaling Technology, Inc. These restrictions do not limit the right to use information legally obtained from a third party source. This document is issued as a REFERENCE COPY and is not revision controlled, unless otherwise indicated by Cell Signaling Technology, Inc. internal procedures.