CtrlS

29 January 2022

PHYSICAL& ENVIRONMENTAL SECURITY POLICY

Physical Security

CTRLS DATACENTERS LTD

DOCUMENT CONTROL:

Preparation

Draft	**Author**	**Date**
1.0	Krupakar	16/04/2013
1.1	Sudheer	24/09/2013
1.2	Sudheer G	19/03/2014
1.3	Soudha Rahman	3/4/2015
1.4	Deepthi Naidu	2/01/2016
1.5	M.Venkataniranjan	8/06/2016
1.6	M.Venkataniranjan	8/01/2017
1.7	M.Venkataniranjan	06/01/2018
1.8	M.Venkataniranjan	10/10/2018
1.8	M.Venkataniranjan	05/01/2019
1.8	M.Venkataniranjan	02/01/2020
1.8	Vasanth G	30/12/2020
1.8	Sandeep Tomer	31/12/2021
1.8	Sandeep Tomer	29/01/2022

Classification	**Storage Location**
Confidential	Shared folder

Review & Approval

Reviewer & Approver	**Version**	**Date**	**Reviewed Draft Version**
RS Prasad Rao	1.0	16/04/2013	1.0
RS Prasad Rao	1.1	24/09/2013	1.1
RS Prasad Rao	1.2	19/03/2014	1.2
RS Prasad Rao	1.3	31/03/2015	1.3
RS Prasad Rao	1.4	1/02/2016	1.4
RS Prasad Rao	1.5	8/06/2016	1.5
RS Prasad Rao	1.6	16/01/2017	1.6
RS Prasad Rao	1.7	06/01/2018	1.7
RS Prasad Rao	1.8	10/10/2018	1.8
RS Prasad Rao	1.8	07/01/2019	1.8
RS Prasad Rao	1.8	03/01/2020	1.8
RS Prasad Rao	1.8	01/01/2021	1.8

V Surender Reddy	1.8	31/12/2021	1.8
V Surender Reddy	1.8	29/01/2022	1.8

Release

Release Version	**Date Released**
1.0	16/04/2013
1.1	24/09/2013
1.2	19/03/2014
1.3	31/03/2015
1.4	1/02/2016
1.5	8/06/2016
1.6	16/01/2017
1.7	6/01/2018
1.8	10/10/2017
1.8	07/01/2019
1.8	03/01/2020
1.8	31/12/2021
1.8	29/01/2022

Distribution List

Name	**Designation**	**Department**
COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	**Change Reason**	**Effective Date**
1.1	Structured Table of contents, re-structured sections and Formatted with version control	24/09/2013
1.2	Added statement of Confidentiality & Reviewed	19/03/2014
1.3	Reviewed and minor update	31/03/2015
1.4	Reviewed and No update	1/02/2016
1.5	Reviewed and Updated version	8/06/2016
1.6	Reviewed and Updated version and scope	16/01/2017
1.7	Reviewed with no update	6/01/2018
1.8	Reviewed and added Training section - 5, Review of the policy section -6	10/10/2018
1.8	No updates	05/01/2019

1.8	No updates	03/01/2020
1.8	No updates	30/12/2020
1.8	No updates	31/12/2021
1.8	Reviewed and No updates	29/01/2022

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating CtrlS Datacenters Ltd. The information contained herein is to be considered confidential. Customer, by receiving this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by CtrlS Datacenters Ltd.

TABLE OF CONTENTS

1 INTRODUCTION

The Physical and Environmental Security Policy is in place to ensure that necessary controls are in place to reduce the risk of theft and / or damage to information and information processing facilities (including work areas and computer environment). The physical access shall be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to information, information processing facilities, media and other sensitive areas.

2 OBJECTIVE

The objective of this policy is to establish procedures and controls to prevent unauthorized physical access, damage, and interference to the CtrlS premises and information and to ensure physical access restrictions and environmental security to CtrlS on basis of business and security requirements.

3 SCOPE

This procedure shall apply to all employees of CtrlS , its contractors, subcontractors, associated third parties who are users of CtrlS services or who have access to CtrlS facility..

4 POLICY STATEMENT

CtrlS shall enforce appropriate individuals to enforce appropriate entry controls and authentication procedures that shall ensure that only authorized personnel are allowed entry into areas that house critical or sensitive information or information processing resources that host the processing of critical or sensitive information. This shall also include any visitors, contractors, or technicians who may have access to the premises. CtrlS shall also implement an appropriate level of controls to ensure that environmental exposures like fire, water, flood, temperature etc. are adequately controlled. This Policy document shall supplement the Security Companion document maintained at CtrlS . (*Refer: Security Companion - released earlier by CtrlS Administration department).*

4.1 Understanding and Protecting the Premise

- CtrlS security perimeter shall be clearly defined and appropriate level of controls and security shall be implemented based on the security requirements for siting and strength of perimeter and based on the results of risk assessment carried out.
- CtrlS shall ensure that the perimeters of the CtrlS premises shall be physically sound;
    - Ensuring that there is no gap in the perimeter or areas where a break-in could occur.
    - Ensuring that external walls of the premises shall be of solid construction and all the external doors shall be suitably protected against unauthorized access with control mechanisms like burglar alarms, bars, locks etc.
    - Doors and windows shall be locked when unattended and external protection shall be considered for windows, particularly at ground level.
    - Additional security controls shall be implemented in the areas identified as vulnerable, as a result of risk assessment.

4.2 Entry restrictions into and within premises

- Only employees, whose job description demand access to CtrlS shall be allowed to enter the premises.
- Visitors' entry into CtrlS premises shall be restricted. Appropriate security validations and checks such as verifying the identity of the visitor, checking the belongings, and bags etc. shall be carried out.
- Access to server and equipment rooms shall be controlled and restricted to authorized personnel who shall need access to perform their defined roles and responsibilities.
- Use of authentication mechanisms like proximity cards, biometric systems shall be considered for server rooms, collocation areas, Internet Data Center areas, Data centre and the area where critical systems and applications are housed.
- Visitors and third parties shall not be permitted access to the server rooms, collocation areas, Internet Data Center areas, Data centre and the area where critical systems and applications are housed. If need be (servicing, maintenance, audit, housekeeping), visitors shall be escorted by respective teams (IDC team member, Operations team etc.). This arrangement shall exclude employees of outsourcing agency who shall be responsible for owning or operating an information processing facility at CtrlS , but shall carry a proper identification card issued by CtrlS for a specified period.
- All the rules and regulations about parking policy for the site should be adhered to.
- Based on the contractual agreement, all the customer cages access is restricted. With proper justification and necessary approvals, authorized persons shall access the customer cage

4.3 Movement of assets in and out of CtrlS premises

- All assets movements have done inside CtrlS and assets carried out of CtrlS shall be duly authorized and tracked.
- Any personal information storage media such as tapes, DAT drives, floppy drives shall not be allowed to be brought inside CtrlS , unless approved and authorized by Head – Security.
- Any material movement beyond the normal working hours should be intimated in advance to the Physical Security / Administration Department for smooth operations.

4.4 Removal of Property

- CtrlS shall enforce authorization and control procedures that ensure information systems assets such as equipment or software from CtrlS are removed for business purpose only. The appropriate level of authorization shall need to be obtained for removing any CtrlS property.
- All information system equipment containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten before disposal.

4.5 Equipment Security – Equipment Placement & Protection

- Information processing resources shall be located away from hazardous processes or materials.
- Adequate power supplies and auxiliary power supplies shall be provided to Information Systems.

- Adequate protection shall be provided to information and information processing resources against damage from exposure to water, smoke, dust, chemicals, electrical supply interference etc.
- The minimum – security protection activities specified by the vendor/manufacturer of information systems equipment shall be implemented.
- Physical emergency procedures shall be documented. CtrlS personnel shall be trained inappropriate behaviour in emergencies.
- Adequate Siting and protection of equipment to reduce the risks from environmental hazards and unauthorized access and misuse shall be implemented.
- Data storage shall be protected from power failures where appropriate e.g. UPS. This shall be monitored and tested by the ITIS team and the Internet Data Center Department (IDC).
- Data Storage shall be adequately protected from power surges where appropriate e.g. Data Center.
- Power and telecommunications cabling shall be protected from interception or damage where possible.
- Equipment shall be maintained under manufacturer's instructions and or documented procedures to ensure its continued availability and integrity.
- All equipment containing storage media shall be checked to ensure that any sensitive data and licensed software have been removed or securely overwritten before disposal.
- Equipment, information or software shall not be taken off-site without prior authorization from the Departmental Head /Head – Security.

4.6 Security of Electronic Equipments

- All the electronic office equipment including faxes, printers and epabx, shall be physically secured.
- Access to the electronic equipment shall be restricted only to authorized users to ensure that no visitor can gain easy access without notice of the staff.

4.7 Security of Information processing equipment Off-Premises

- Virus controls shall be enabled to protect CtrlS information resources.
- Information processing equipment and media containing sensitive data shall not be left unattended in public places. Portable computers / Laptops carrying sensitive data shall be carried as hand luggage when travelling.
- Off-premises computers, with CtrlS classified information shall be protected with an appropriate form of access protection, e.g. passwords, smart cards, or encryption, to prevent unauthorized access.
- Manufacturers' instructions regarding physical protection of equipment shall be observed at all times.
- Security risks (e.g. damage, theft, eavesdropping) vary considerably between locations and shall be considered in determining the most appropriate security measures.

4.8 Cabling Security

- Power and communication lines servicing CtrlS premise shall be underground, where possible, or subject to adequate alternate protection (concealed wiring). Network cabling shall be protected from unauthorized interception or damage.

4.9 Security of Desktops and Network hubs

- Desktops shall be adequately protected from fire, water, and pollution, damage, and power fluctuations.
- Network hubs shall be secured from fire, heat, dust, and water.

4.10 Power Supplies

- An uninterruptible Power Source (UPS) shall be used to support critical business information processing operations. UPS equipment shall be regularly tested according to the manufacturer's recommendations. Computer hardware shall be protected from electrical surges.
- There shall be a provision to maintain regular power supply within CtrlS .
- Alternate power supply sources shall be present to ensure continuous power supply in the absence of primary power sources.

4.11 Media Handling and Security

(*Refer: ISMS – Media Handling Policy and Procedure and ISMS – Information Labeling and Handling Procedure)*

- Media shall be protected from physical damages like fire, moisture, and magnetic interference.
- All media shall be handled with care and shall be ensured that they are not kept near magnetic material and are not exposed to any extreme heat or pollution.
- A stock or inventory of all the media shall be maintained.
- Media shall be disposed of securely and safely when no longer required.
- Formal procedures for the secure disposal of media shall be established to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.
- Special controls shall be adopted, wherever necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, tamper-evidentnt packaging (which reveals any attempt to gain access).

4.12 Clear Desk & Screen Policy

- CtrlS shall follow clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours.

4.13 Safety against environmental hazards

- CtrlS shall be equipped with systems and controls to mitigate risk arising from potentially harmful environments.

- CtrlS shall install appropriate fire fighting devices at critical locations in order to arrest the fire and to avoid damage to the various resources of CtrlS . – (Shall be integrated with the Building Management System maintained for CtrlS , where possible).
- Safety measures like fire and earthquake evacuation drills shall be carried out at regular intervals.
- Appropriate safety measure shall be taken to avoid loss and damage due to water flooding or inappropriate drainage system within the premises of CtrlS .
- CtrlS shall not keep the backup media and fall back equipment at the main site. Security threats presented by neighbouring premises shall also be evaluated.
- Combustible material shall be stored at a safe distance from the secure area (in consultation with Physical Security and Administration Department)

4.14 Operational Requirements

- The physical premises shall be monitored on an adequate and consistent basis through both manual and automated techniques to prevent and detect unauthorized access, access attempts, and suspicious activity.
- Security personnel shall periodically inspect sensitive areas, as well as vacant areas, in the building manually and with electronic assistance, particularly during non-business hours, and shall log all information relating to issues noted.
- Only authorized maintenance personnel shall carry out repairs and service equipment. Vendor representatives shall be supervised when performing such maintenance activities. (Work Permits for enabling vendors/support personnel to carry out repairs and servicing shall be managed by the Physical Security and Administration Department)

5 TRAINING

- CtrlS shall ensure all team members undergo periodical training outlined in this policy.

6 REVIEW OF THE INFORMATION SECURITY POLICY

- This document will be reviewed and updated on an annual basis or when significant changes occur to the organization systems and information security standards.

7 COMPLIANCE WITH THE POLICY

Compliance with the Physical and Environmental Security Policy and Procedure shall be mandatory. Head Security–CtrlS, assisted by information security forum shall ensure continuous compliance to this policy and procedure within CtrlS . The periodic review shall be conducted by Departmental Heads and shall be reported to Head – Security to verify compliance with this policy and procedure. All employees shall be responsible to inform the Head– Security if any policy breach is discovered or identified.

8 VIOLATION WITH THE POLICY

Any user found to have violated this Physical and Environmental Security Policy and Procedure may be subjected to disciplinary action, up to and including termination of employment.

8.1 Consequences of violation of the Policy

Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets, and
- Other actions as deemed appropriate by Management, Human Resources, and the Legal Department.

9 CONTACT ROLE FOR CLARIFICATION REGARDING THE POLICY

The sponsor of this policy is the Head – Security. Head – Security – CtrlS shall be responsible for the maintenance and accuracy of the policy. Any questions regarding this policy shall be directed to the Head – Information Security.

10 WAIVER CRITERIA

This Policy and Procedure is intended to address information security requirements. Requested waivers shall be formally submitted to the Head – Security including justification and benefits attributed to the waiver for approval. The waiver shall only be used in exceptional situations for communicating non-compliance with the policy for a specific period (subject to a maximum period of 30 days). After the time period, the need for the waiver shall be reassessed and re-approved, if necessary. Waiver shall not be provided for more than three consecutive terms. The waiver shall be monitored to help ensure its concurrence with the specified period and exception.