

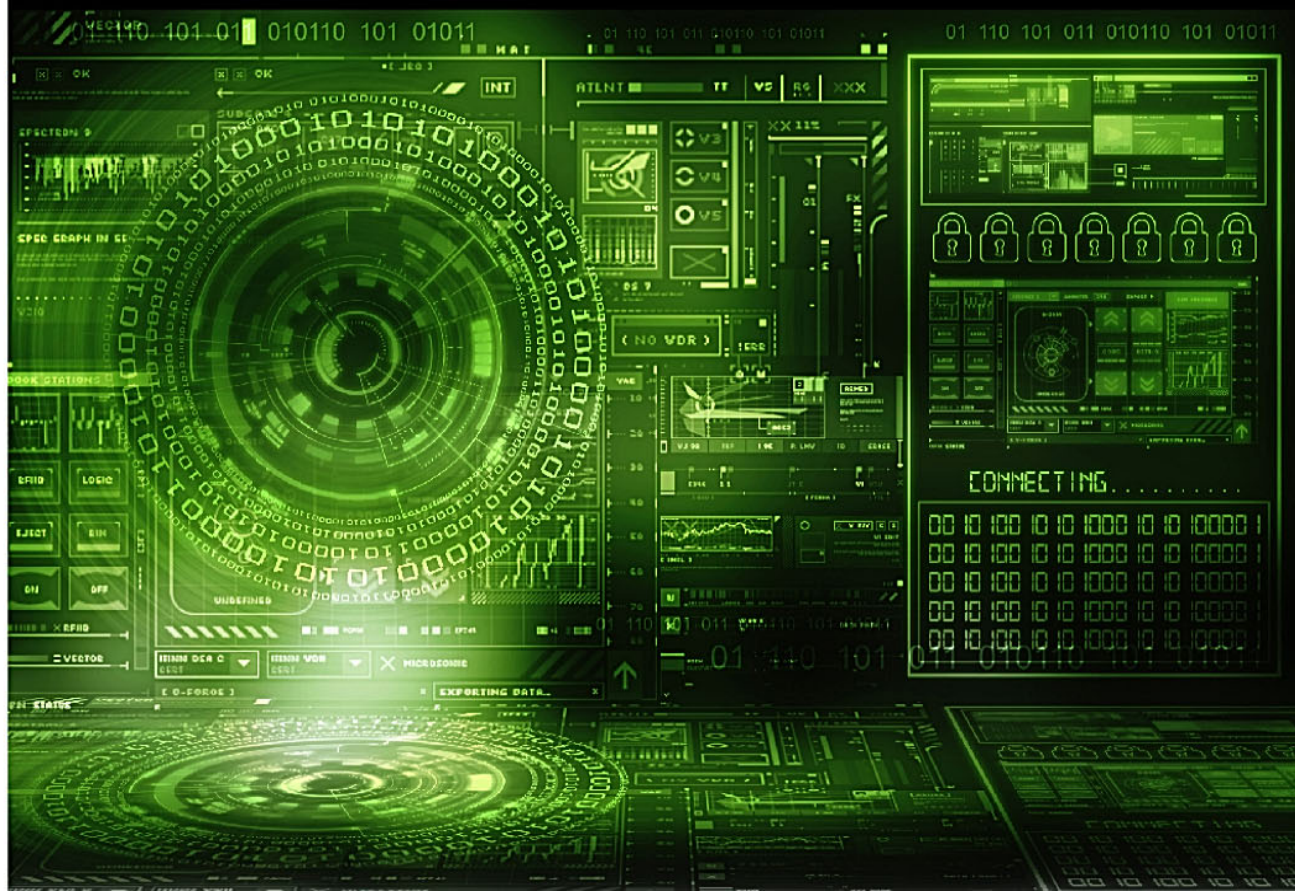
STANDARDS



a BICSI International Standard

BICSI 009-2019

Data Center Operations and Maintenance Best Practices



BICSI 009-2019

Data Center Operations and Maintenance Best Practices

Committee Approval: March 27, 2019

First Published: May 1, 2019



BICSI International Standards

BICSI international standards contain information deemed to be of technical value to the industry and are published at the request of the originating committee. The BICSI International Standards Program subjects all of its draft standards to a rigorous public review and comment resolution process, which is a part of the full development and approval process for any BICSI international standard.

The BICSI International Standards Program reviews its standards at regular intervals. By the end of the fifth year after a standard's publication, the standard will be reaffirmed, rescinded, or revised according to the submitted updates and comments from all interested parties.

Suggestions for revision should be directed to the BICSI International Standards Program, care of BICSI.

Copyright

This BICSI document is a standard and is copyright protected. Except as permitted under the applicable laws of the user's country, neither this BICSI standard nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording, or otherwise, without prior written permission from BICSI being secured.

Requests for permission to reproduce this document should be addressed to BICSI.

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Published by:



BICSI
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA

Copyright © 2019 BICSI
All rights reserved
Printed in U.S.A.

Notice of Disclaimer and Limitation of Liability

BICSI standards and publications are designed to serve the public interest by offering information communication and technology systems design guidelines and best practices. Existence of such standards and publications shall not in any respect preclude any member or nonmember of BICSI from manufacturing or selling products not conforming to such standards and publications, nor shall the existence of such standards and publications preclude their voluntary use, whether the standard is to be used either domestically or internationally.

By publication of this standard, BICSI takes no position respecting the validity of any patent rights or copyrights asserted in connection with any item mentioned in this standard. Additionally, BICSI does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standard or publication. Users of this standard are expressly advised that determination of any such patent rights or copyrights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard does not purport to address all safety issues or applicable regulatory requirements associated with its use. It is the responsibility of the user of this standard to review any existing codes and other regulations recognized by the national, regional, local, and other recognized authorities having jurisdiction (AHJ) in conjunction with the use of this standard. Where differences occur, those items listed within the codes or regulations of the AHJ supersede any requirement or recommendation of this standard.

All warranties, express or implied, are disclaimed, including without limitation, any and all warranties concerning the accuracy of the contents, its fitness or appropriateness for a particular purpose or use, its merchantability and its non-infringement of any third-party's intellectual property rights. BICSI expressly disclaims any and all responsibilities for the accuracy of the contents and makes no representations or warranties regarding the content's compliance with any applicable statute, rule, or regulation.

BICSI shall not be liable for any and all damages, direct or indirect, arising from or relating to any use of the contents contained herein, including without limitation any and all indirect, special, incidental, or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based upon breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. The foregoing negation of damages is a fundamental element of the use of the contents hereof, and these contents would not be published by BICSI without such limitations.

TABLE OF CONTENTS

	PREFACE	xi
1	Introduction	1
1.1	General	1
1.2	Purpose	1
1.2.1	ICT Operations	1
1.2.2	Facilities Operations	2
1.2.3	Data Center Management	2
1.3	Impact of Redundancy on Operations and Maintenance Procedures	2
1.3.1	Standard Operating Procedures	3
1.3.2	Maintenance Operating Procedures	3
1.3.3	Emergency Operating Procedures	3
1.4	Categories of Criteria	3
2	Scope	5
3	Required Standards and Documents	7
4	Definitions, Acronyms, Abbreviations, and Units of Measurement	9
4.1	Definitions	9
4.2	Acronyms and Abbreviations	16
4.3	Units of Measurement	16
5	Governance and Assessment	17
5.1	Introduction	17
5.1.1	Public Governance	17
5.1.2	Private Governance	17
5.2	Compliance	17
5.2.1	Documentation	18
5.3	Voluntary Assessment Programs	18
5.3.1	Overview	18
5.4	Types of Assessments	18
5.4.1	Introduction	18
5.4.2	Risk Assessment	18
5.4.3	Data Center Operations and Maintenance Assessment	19
5.4.4	Security Assessment	19
6	Standard Operating Procedures	21
6.1	Introduction	21
6.2	BICSI Class Definition and Standard Operating Procedures	21
6.3	ICT Cut-overs, Technology Refresh and Migration	21
6.3.1	Cut-Overs	21
6.3.2	Change Control Process	21
6.4	Work Orders	22
6.4.1	Introduction	22
6.4.2	Data Center Installation Work Order	22
6.4.3	Example of a Data Center Work Order Process for ITE	24

6.5	Work Safety	25
6.5.1	Scope.....	25
6.5.2	Safety Planning.....	25
6.5.3	Safety Meetings and Briefings.....	26
6.5.4	Emergencies.....	27
6.5.5	Electrical Safety.....	28
6.5.6	Mechanical Safety.....	30
6.5.7	Personal Protective Equipment (PPE).....	31
6.5.8	Work Place Safety Training.....	33
6.5.9	Accident Reporting.....	36
6.6	Storage, Staging, and Related Tasks.....	38
6.6.1	Storage.....	38
6.6.2	Staging.....	38
6.6.3	Packing and Unpacking.....	38
6.6.4	Manufacturer Testing.....	38
6.6.5	End User Burn-In.....	38
6.7	Interface with Data Center Users.....	38
6.7.1	Data Center Service.....	38
6.7.2	Correspondences (Interface procedures).....	40
6.7.3	Facility Operations.....	41
6.7.4	Facility Reports.....	41
6.7.5	Periodical Meetings.....	42
6.7.6	External Personnel Access.....	43
6.8	Equipment Delivery and Shipments	43
6.8.1	Materials Management.....	43
6.8.2	Procurement Processes.....	43
6.8.3	Shipping Considerations.....	43
6.8.4	Receiving Materials.....	44
6.8.5	Handling Hazardous Materials.....	44
7	Security	45
7.1	Introduction	45
7.2	Risk and Threat Assessment.....	46
7.3	Regulatory and Insurance Considerations	46
7.3.1	Introduction.....	46
7.3.2	Regulations or Laws Affecting Security.....	46
7.4	Data Center Security Plan	47
7.4.1	Introduction.....	47
7.4.2	General Recommendations.....	47
7.4.3	Physical Security Plan.....	47
7.4.1	Cyber/IT Security Plan.....	48
7.5	Physical Security Systems	49
7.5.1	Access Control.....	49
7.5.2	Badging and Identification.....	53
7.5.3	Signage and Display Policy and Procedures.....	54
7.5.4	Fire Prevention, Detection and Suppression.....	54
7.5.5	Video Surveillance.....	54
7.5.6	Monitoring and Alarms.....	54

7.6	Material Control and Loss Prevention	55
7.6.1	Introduction	55
7.6.2	Recommendations	55
7.6.3	Classification and Confidentiality of Sensitive Resources	56
7.6.4	Hazardous Material Storage	56
7.6.5	Disposal of Media and Printed Material	56
7.6.6	Theft	56
7.7	Data Center Personnel	56
7.7.1	Introduction	56
7.7.2	Hiring of Personnel	57
7.7.3	Reporting	57
7.7.4	Terminations of Personnel	57
7.8	Building Site	58
7.8.1	Site Access and Egress	58
7.8.2	Security Guards	58
7.8.3	Office Areas	59
7.9	Assessments	59
7.10	Computer Room and Critical Facility Areas Special Considerations	59
7.10.1	Requirements	59
7.10.2	Recommendations	59
7.11	Cyber/IT Security Policy and Procedures	60
7.11.1	Introduction	60
7.11.2	Passwords	60
7.11.3	Information Control	60
7.12	Event Response	60
7.12.1	Physical Security	60
7.12.2	Cyber/IT Security Event Response	61
7.12.3	Post-Mortem Processes and Policies	61
8	Maintenance Operating Procedures	63
8.1	Introduction	63
8.1.1	BICSI Class Definition and Maintenance Procedures	63
8.1.2	Maintenance Activities and Risk	63
8.2	Maintenance Document Library	64
8.2.1	Introduction	64
8.2.2	Documentation	64
8.2.3	Maintenance Record Keeping	65
8.3	Maintenance Management	65
8.3.1	Introduction	65
8.3.2	Maintenance Types	65
8.4	Equipment Maintenance Plan	68
8.4.1	Introduction	68
8.4.2	Maintenance Tasks for EMPs	69
8.4.3	EMP Elements	69
8.5	Maintenance Contracts	70
8.5.1	Introduction	70
8.5.2	Requirements	70
8.5.3	Recommendations	70
8.5.4	Maintenance Specification	71
8.6	Routine Patrols and Inspections	72

8.7	Power Systems	72
8.7.1	Introduction.....	72
8.7.2	Requirements.....	72
8.7.3	General Recommendations.....	73
8.7.4	Grounding and Lightning Protection.....	73
8.7.5	Utility Input Switchgear.....	74
8.7.6	Distribution Systems.....	74
8.7.7	Mechanical Equipment Power Supply.....	74
8.7.8	Control Systems.....	74
8.7.9	Transfer Switches.....	74
8.7.10	UPS (Uninterruptable Power Supply).....	75
8.7.11	Backup and Emergency Power Systems.....	76
8.8	ITE Moves, Adds and Changes	77
8.8.1	Equipment Maintenance Outages.....	77
8.9	Cooling Systems.....	78
8.9.1	Introduction.....	78
8.9.2	Preventative Maintenance Program.....	79
8.9.3	Maintenance and Replacement of Components.....	80
8.10	Computer Room Airflow	84
8.10.1	Introduction.....	84
8.10.2	Blanking Panels.....	84
8.10.3	Rail Blanking.....	84
8.10.4	Cable Access Holes.....	84
8.10.5	External Containment Functionality.....	85
8.10.6	Cable Hygiene.....	85
8.10.7	Access Floor System Maintenance.....	85
8.10.8	Floor Tile Placement.....	86
8.10.9	Room Sensors.....	86
8.10.10	Recommendations.....	86
8.11	Cabling Systems Maintenance.....	86
8.11.1	Introduction.....	86
8.11.2	Recommendations.....	87
8.12	Building Systems.....	87
8.12.1	Fire Detection, Suppression and Notification.....	87
8.12.2	Monitoring and Management Systems.....	88
8.12.3	Physical Security and Access Control.....	88
8.13	Area and Physical Space Maintenance.....	89
8.14	Spare Parts and Consumables.....	89
8.14.1	Consideration.....	89
8.14.2	Management of Spares and Spare Parts.....	90
8.15	IT Network and Telecommunication Systems.....	90
9	Emergency Operating Procedures.....	91
9.1	Introduction.....	91
9.2	Response Documentation.....	91
9.3	Internal Data Center Events.....	91
9.3.1	Equipment Failures.....	91
9.3.2	Critical Services Failures.....	92
9.3.3	Operational Troubles.....	92
9.4	On-Site Events.....	93
9.4.1	Initial Event Response.....	93
9.4.2	Upon Event Resolution.....	94

9.5	Offsite Events	94
9.5.1	Initial Event Response.....	94
9.5.2	Upon Event Resolution.....	94
9.6	Emergency Response to Natural Disasters	95
9.6.1	Initial Event Response.....	95
9.6.2	Upon Event Resolution.....	95
9.7	Emergency Response to Physical Security Breach	95
9.8	Emergency Response to Personal Injury	96
9.8.1	Initial Event Response.....	96
9.9	Disaster Recovery	96
9.9.1	Introduction.....	96
9.9.2	Plan.....	96
9.9.3	Personnel.....	97
9.9.4	Essential Disaster Recovery Components.....	97
9.9.5	Testing of Disaster Recovery Plans.....	98
9.9.6	Chemical, Biological, Radiological, Nuclear and Explosives.....	98
10	Management	99
10.1	Operations Management Overview	99
10.1.1	Service Operations.....	99
10.1.2	Service Desk.....	100
10.1.3	IT Service Management (ITSM).....	101
10.1.4	IT Operations Management.....	102
10.1.5	Technical Management.....	103
10.1.6	Application Management.....	103
10.1.7	IT Security Management.....	104
10.1.8	Management of Facility Operations.....	104
10.2	Management Tools	105
10.2.1	Overview.....	105
10.2.2	DCIM.....	105
10.2.3	Infrastructure Asset Management.....	113
10.2.4	Configuration Management Data Base.....	114
10.2.5	Building Management Systems (BMS).....	116
10.2.6	Automated Infrastructure Management (AIM) Systems.....	117
10.3	Operational Management Modules	119
10.3.1	Introduction.....	119
10.3.2	Asset Management Module.....	119
10.3.3	Network Discovery Module.....	120
10.3.4	Connectivity Management Module.....	120
10.3.5	Power Management Module.....	120
10.3.6	Capacity Planning Module.....	121
10.3.7	Dashboard Module.....	122
10.3.8	Workflow Module.....	123
10.3.9	End-to-End Resource Management.....	123
10.4	Service Provider Management	123
10.4.1	Introduction.....	123
10.4.2	Cloud Service Models.....	123
10.4.3	Cloud Installation Models.....	124
10.4.4	Cloud Considerations.....	124
10.5	Metrics and Measurement	125
10.5.1	Introduction.....	125

10.6	Change Management, Change Control, and Documentation	126
10.6.1	Introduction.....	126
10.6.2	Scope.....	127
10.6.3	Requirements for Change Management Procedures	127
10.6.4	Types of Changes in a Data Center.....	128
10.6.5	Risk Classifications.....	128
10.6.6	Change Review Board (CRB).....	129
10.7	Data Center Security	129
10.7.1	Hardware Security Technologies	130
10.7.2	Firmware Security Technologies	130
10.7.3	Virtualization Security Technologies.....	130
10.7.4	Other Security Technologies.....	130
10.8	Operations Organizational Structure	131
10.8.1	Introduction.....	131
10.9	Training.....	132
10.9.1	Facility Systems	132
Appendix A	Related Documents (Informative).....	135

INDEX OF FIGURES

Section 6	Standard Operating Procedures	
Figure 6-1	Example of a LOTO Electrical Safety Form.....	29
Figure 6-2	Example of a LOTO Justification Form.....	30
Figure 6-3	Example LOTO Custody of Equipment Flow Chart.....	35
Figure 6-4	Example of an Accident / Incident Reporting Form.....	37
Section 7	Security	
Figure 7-1	Security Measures	45
Figure 7-2	Levels of Access Control	50
Figure 7-3	Example of a Visually Distinctive Expired Badge.....	54
Section 8	Maintenance Operating Procedures	
Figure 8-1	Risk During Normal vs Maintenance Modes	64
Figure 8-2	Example of Measurements Points for Vibrational Testing	68
Section 10	Management	
Figure 10-1	DCIM System Outline Configuration	107
Figure 10-2	Configuration Management Data Base (CMDB) Model.....	115
Figure 10-3	Data Center Ownership Models	124
Figure 10-4	Data Center Metrics	125

This page intentionally left blank

PREFACE

Revision History

May 1, 2019 First publication of this standard, titled BICSI 009-2019, *Data Center Operations and Maintenance Best Practices*

Translation Notice

This standard may have one or more translations available as a reference for the convenience of its readers. As that act of translation may contain inconsistencies with the original text, if differences between the translation and the published English version exist, the English text shall be used as the official and authoritative version.

This page intentionally left blank

1 Introduction

1.1 General

This standard is written with the expectation that the reader is familiar with the different facets of operating and maintaining data center IT systems and supporting facility systems. The reader should understand from which role and point of view he or she intends to use this document (e.g., information technology, facilities, other corporate internal or external to the owner). Refer to Sections 1.2.1 –1.2.3 below.

1.2 Purpose

This standard provides a reference of common terminology and operating practices. It is not intended to be used by managers, administrators or technicians as their sole reference or as a step-by-step operations guide, but may be used by such persons to determine operation requirements in conjunction with the data center owner, management, administrators, technicians, and in the case of data center outsourcing vendors - customers.

This standard is intended primarily for:

- Data center owners
- Data center management
- Data center operations
- Project managers
- Information and communications technology (ICT) project managers, technicians and system administrators

Additionally, individuals in the following groups are also served by this standard.

1.2.1 ICT Operations

1.2.1.1 ICT Representatives

ICT operations that may use BICSI 009 to develop policies and procedures include:

- Application developers
- Server, storage and network system administrators
- Network Security
- ICT network cabling technicians
- Network operations center (NOC) technicians
- Rack & stack technicians
- IT service desk support and knowledge management
- Change management
- Project management
- Risk management

1.2.1.2 ICT Groups

Each of the ICT representatives listed above may work within one or more of the following areas of responsibility:

- Planning and design
- Intake and transition
- Release management
- Change management
- General operations
- Risk management

ICT operations should coordinate policies and procedures with Facility operations to ensure the policies and procedures of one discipline does not introduce unnecessary risk on the data center operations.