



Full Policy
available upon
request (142 pages)

Information Security Policy

Version 3.0
February 16, 2017

Jefferson County Local Development Corporation
800 Starbuck Ave
Suite 800
Watertown, NY 13601

Table of Contents

Introduction.....	9
Overview	9
Scope.....	9
Goals	9
Intent.....	10
Implementation	10
Revision History	10
I. Acceptable Use Policy	11
1.0 Overview	11
2.0 Purpose	11
3.0 Scope.....	11
4.0 Policies	11
4.1 Network Access	11
4.2 Web Browsing and Internet Usage	12
4.3 Unacceptable Use	13
4.4 Monitoring and Privacy	15
4.5 Responsible Computer and Network Use.....	16
4.6 Reporting of a Security Incident	17
4.7 Applicability of Other Policies	17
5.0 Enforcement	17
II. Password Policy	18
1.0 Overview	18
2.0 Purpose	18
3.0 Scope.....	18
4.0 Policies	18
4.1 Construction	18
4.2 Confidentiality	19
4.3 Change Frequency.....	19
4.4 Incident Reporting	20
4.5 Applicability of Other Policies	20
5.0 Enforcement	20
III. Remote Access Policy	21
1.0 Overview	21
2.0 Purpose	21
3.0 Scope.....	21
4.0 Policies	21
4.1 Remote Access Client Software	21
4.2 Remote Network Access	22

Attached

4.3 Idle Connections	23
4.4 Prohibited Actions	23
4.5 Use of non-company-provided Systems.....	23
4.6 Applicability of Other Policies	24
5.0 Enforcement	24
IV. Confidential Data Policy	25
1.0 Overview	25
2.0 Purpose	25
3.0 Scope.....	25
4.0 Policies	25
4.1 Data Classification.....	25
4.2 Treatment of Confidential Data.....	26
4.3 Examples of Confidential Data.....	28
4.4 Use of Confidential Data	29
4.5 Sharing Confidential Data with Third Parties	29
4.6 Receiving Confidential Data from Third Parties.....	30
4.7 Security Controls for Confidential Data.....	30
4.8 Emergency Access to Data.....	32
4.9 Applicability of Other Policies	33
5.0 Enforcement	33
V. Mobile Device Policy	34
1.0 Overview	34
2.0 Purpose	34
3.0 Scope.....	34
4.0 Policies	34
4.1 Physical Security	34
4.2 Data Security	35
4.3 Connecting Mobile Computers to Unsecured Networks.....	36
4.4 General Guidelines.....	36
4.5 Audits.....	37
4.6 Applicability of Other Policies	37
5.0 Enforcement	37
VI. Retention Policy.....	38
1.0 Overview	38
2.0 Purpose	38
3.0 Scope.....	38
4.0 Policies	39
4.1 Reasons for Data Retention.....	39
4.2 Data Duplication	39

4.3 Retention Requirements	39
4.4 Retention of Encrypted Data	40
4.5 Data Destruction	40
4.6 Applicability of Other Policies	41
5.0 Enforcement	41
VII. Email Policy	42
2.0 Purpose	42
3.0 Scope	42
4.0 Policies	42
4.1 Proper Use of Company Email Systems	42
4.2 External and/or Personal Email Accounts	46
4.3 Confidential Data and Email	47
4.4 Company Administration of Email	47
4.5 Prohibited Actions	51
4.6 Applicability of Other Policies	52
5.0 Enforcement	53
VIII. Backup Policy	54
1.0 Overview	54
2.0 Purpose	54
3.0 Scope	54
4.0 Policies	54
4.1 Identification of Critical Data	54
4.2 Data to be Backed Up	55
4.3 Backup Frequency	55
4.4 Off-Site Rotation	56
4.5 Backup Storage	56
4.6 Backup Retention	56
4.7 Restoration Procedures & Documentation	57
4.8 Restoration Testing	57
4.9 Expiration of Backup Media	57
4.10 Applicability of Other Policies	58
5.0 Enforcement	58
IX. Network Access and Authentication Policy	59
1.0 Overview	59
2.0 Purpose	59
3.0 Scope	59
4.0 Policies	60
4.1 Account Setup	60
4.2 Account Access Levels	61

4.3 Account Use.....	61
4.4 Account Termination	62
4.5 Network Authentication Requests.....	62
4.6 Database Authentication Requests.....	63
4.7 Use of Passwords.....	63
4.8 Screensaver Passwords	63
4.9 Minimum Configuration for Access.....	63
4.10 Encryption of Login Credentials	64
4.11 Failed Login Attempts	64
4.12 Alternate Authentication Mechanisms	64
4.13 Applicability of Other Policies.....	65
5.0 Enforcement	65
X. Incident Response Policy	66
1.0 Overview	66
2.0 Purpose	66
3.0 Scope.....	66
4.0 Policies	66
4.1 Types of Incidents	66
4.2 Preparation.....	67
4.3 Confidentiality	68
4.4 Electronic Incidents.....	68
4.5 Physical Incidents.....	70
4.6 Hybrid Incidents.....	71
4.7 Notification.....	72
4.8 Managing Risk	73
4.9 Business Recovery and Continuity Planning.....	74
4.10 Applicability of Other Policies.....	77
5.0 Enforcement	77
XI. External Connection Policy	78
1.0 Overview	78
2.0 Purpose	78
3.0 Scope.....	78
4.0 Policies	79
4.1 Encryption	79
4.2 Authentication.....	79
4.3 Implementation	79
4.4 Management	79
4.5 Logging and Monitoring	80
4.6 Encryption Keys	80

4.7 Managing Risk	80
4.8 Restricting Third Party Access.....	80
4.9 Applicability of Other Policies	81
5.0 Enforcement	81
XII. Guest Access Policy	82
1.0 Overview	82
2.0 Purpose	82
3.0 Scope.....	82
4.0 Policies	82
4.1 Granting Guest Access.....	82
4.2 Guest Access Infrastructure Requirements	83
4.3 Restrictions on Guest Access	83
4.4 Monitoring of Guest Access.....	84
4.5 Applicability of Other Policies	84
5.0 Enforcement	84
XIII. Wireless Access Policy	85
1.0 Overview	85
2.0 Purpose	85
3.0 Scope.....	85
4.0 Policies	85
4.1 Physical Guidelines	85
4.2 Configuration and Installation.....	86
4.3 Accessing Confidential Data	87
4.4 Inactivity.....	88
4.5 Wireless Scans	88
4.6 Audits.....	88
4.7 Wireless Access Point Inventory	89
4.8 Applicability of Other Policies	89
5.0 Enforcement	89
XIV. Network Security Policy	90
1.0 Overview	90
2.0 Purpose	90
3.0 Scope.....	90
4.0 Policies	90
4.1 Network Device Authentication	90
4.2 Logging	93
4.3 Audit Trails	94
4.4 Firewalls	96
4.5 Networking Hardware.....	98

4.6 Network Servers	100
4.7 Intrusion Detection/Intrusion Prevention.....	101
4.8 File Integrity Monitoring	101
4.9 Security Testing	101
4.10 Disposal of Information Technology Assets.....	105
4.11 Network Compartmentalization	105
4.12 Network Documentation.....	106
4.13 Antivirus/Anti-Malware	107
4.14 Software Use Policy.....	109
4.15 Software/Application Development Policy	109
4.16 Maintenance Windows and Scheduled Downtime	111
4.17 Change Management	111
4.18 Suspected Security Incidents	112
4.19 Redundancy	112
4.20 Manufacturer Support Contracts.....	113
4.21 Security Policy Management	113
4.22 Applicability of Other Policies.....	115
5.0 Enforcement	115
XV. Encryption Policy	116
1.0 Overview	116
2.0 Purpose	116
3.0 Scope.....	116
4.0 Policies	116
4.1 Applicability of Encryption	116
4.2 Encryption Key Management	118
4.3 Acceptable Encryption Algorithms.....	119
4.4 Legal Use	120
4.5 Applicability of Other Policies	120
5.0 Enforcement	120
XVI. Outsourcing Policy	121
1.0 Overview	121
2.0 Purpose	121
3.0 Scope.....	121
4.0 Policies	121
4.1 Deciding to Outsource.....	121
4.2 Outsourcing Core Functions	122
4.3 Evaluating a Provider	122
4.4 Security Controls.....	123
4.5 Outsourcing Contracts.....	123

4.6 Access to Information	123
4.7 List of Providers	124
4.8 Applicability of Other Policies	124
5.0 Enforcement	124
XVII. Physical Security Policy	125
1.0 Overview	125
2.0 Purpose	125
3.0 Scope.....	125
4.0 Policies	126
4.1 Choosing a Site	126
4.2 Security Zones.....	126
4.3 Access Controls	127
4.4 Physical Data Security	128
4.5 Physical System Security	129
4.6 Fire Prevention	131
4.7 Entry Security	131
4.8 Applicability of Other Policies	132
5.0 Enforcement	132
Appendix A: Policy Acceptance Form.....	134
Appendix B: Definitions.....	135

Introduction

Overview

This security policy was created to communicate the requirements for secure use of company resources, and represents Jefferson County Local Development Corporation's strategy for how it will implement Information Security principles and technologies. This security policy differs from security processes and procedures, in that the policy provides both high level and specific guidelines on how the Company is to protect its data, but does not specify exactly how that is to be accomplished. This provides leeway to choose which security devices and methods are best in consideration of all factors. This policy is technology and vendor independent, as its intent is to set policy only, which can then be implemented in any manner that accomplishes the specified goals.

Scope

The security policy covers Jefferson County Local Development Corporation's information systems and resources. Perhaps more importantly, it covers the Company data stored on these systems as well as any backups or hardcopies of this data.

Where credit card data is stored or transmitted (i.e., the cardholder data environment), more restrictive requirements will apply. Thus, Jefferson County Local Development Corporation should limit the scope of the cardholder data environment to the fullest extent possible.

Goals

The goals of this security policy are to accomplish the following:

1. To allow for the confidentiality and privacy of Jefferson County Local Development Corporation's information.
2. To provide protection for the integrity of Jefferson County Local Development Corporation's information.
3. To provide for the availability of Jefferson County Local Development Corporation's information.

This is commonly referred to as the "CIA Triad" of Confidentiality, Integrity, and Availability, an approach which is shared by all major security regulations and standards. Additionally, this approach is consistent with generally-accepted industry best practices for security management.

Intent

This security policy indicates senior management’s commitment to maintaining a secure network, which allows the IT Staff to do a more effective job of securing Jefferson County Local Development Corporation’s information assets.

A security policy may also provide legal protection to Jefferson County Local Development Corporation, by specifying exactly how users can and cannot use the network, how they should treat confidential information, and the proper use of encryption.

It is the intent of this security policy to clearly communicate the requirements necessary for compliance with any applicable regulations, specifically the Payment Card Industry Data Security Standard Version 3.1 (PCI DSS 3.1), as well as any data confidentiality agreements with third parties.

Implementation

This policy requires the appointment of an Information Security Manager, who will be responsible for implementation and ongoing security administration. Specific guidance on this position can be found within this document. The Information Security Manager doesn’t necessarily need to be an independent position, but can be a designation fulfilled by an existing employee (i.e., the IT Manager) as long as that employee has the authority to hold a management role, and the resources and abilities to commit to the position. This policy must be implemented with full support of management and/or the executive team.

Policies designated as “End User” policies must be distributed to and formally accepted in writing by the users. Specific guidance regarding security policy implementation and ongoing management can be found within this document.

Revision History

<u>Revision</u>	<u>Date</u>	<u>Notes</u>
Revision 1.0	2/10/2012	First Revision for PCI DSS 2.0 compliance
Revision 2.0	1/24/2014	Revised for PCI DSS 3.0 compliance
Revision 3.0	5/15/2015	Revised for PCI DSS 3.1 compliance