

**Security Plan**  
**for**  
**The State of Indiana**  
**Case Management and**  
**Labor Exchange System**

**November 3, 2022**



---

**SIGNATURE PAGE**

---

Approver Name	Role	Signature	Date

---

**CHANGE HISTORY**

---

Version Number	Date	Contributor	Approved by	Approved Date	Description

# Table of Contents

<b>INTRODUCTION.....</b>	<b>1</b>
<b>1 SECURITY PLAN OUTLINE.....</b>	<b>2</b>
<b>2 SECURITY ARCHITECTURE.....</b>	<b>4</b>
<b>3 MULTI LAYERED SECURITY DEFENSES .....</b>	<b>6</b>
<b>4 INFRASTRUCTURE PROTECTION .....</b>	<b>10</b>
4.1 Security Information and Event Management (SIEM) .....	10
4.2 Centralized Security Management .....	11
4.3 Network Perimeter Protection and Intrusion Detection.....	12
4.3.1 Firewall Provisioning.....	13
4.3.2 Intrusion Protection.....	14
4.3.3 Advanced Threat Detection.....	15
4.3.4 Data Loss Prevention (DLP).....	16
4.3.5 Active Data and Trend Analysis .....	16
4.4 Endpoint and Server Protection .....	17
4.5 Internal Network Protection .....	18
4.6 Physical Security of Geographic Solutions Infrastructure .....	19
4.6.1 Access Controls and Equipment .....	19
4.6.2 Visitor and Authorized Personnel Access Control .....	20
4.6.3 Workstation & Internal Network Protection .....	21
<b>5 DATA SECURITY - SECURING CLIENT INFORMATION .....</b>	<b>21</b>
5.1 Protecting Data at Rest and in Use .....	21
5.2 Protecting Data in Transit .....	23
5.3 Web Services Authentication and Encryption .....	23
5.4 Database Access Protection .....	24
5.5 Data Encryption.....	25
5.5.1 Hardware Encryption.....	25

5.5.2	Software Encryption .....	25
5.5.3	FTP Encryption .....	26
5.5.4	Backup Encryption .....	26
<b>6</b>	<b>APPLICATION PROTECTION .....</b>	<b>26</b>
6.1	Architecture and Code Design Standards and Best Practices .....	26
6.1.1	SANS Top 25 Most Dangerous Programming Errors .....	27
6.2	Strong Application Access Controls .....	32
6.2.1	Application User Authentication .....	32
6.2.2	Single Sign On .....	33
6.2.3	Maintaining Credential Security .....	33
6.2.4	Network User Authentication .....	35
6.2.5	Strong Data Access Controls .....	36
6.3	Full Role-Based Security Model .....	38
6.4	Full Audit Trail .....	40
6.4.1	Audit Logs .....	41
6.4.2	Transaction Logging .....	41
<b>7</b>	<b>ORGANIZATIONAL PROTECTION .....</b>	<b>42</b>
7.1	Strict Security Policies and Procedures .....	42
7.1.1	Geographic Solutions Password Policy .....	45
7.1.2	Sanitation and Destruction of Sensitive Information .....	46
7.2	Background Screening .....	47
7.3	Security Training and Education .....	47
7.4	Risk Management .....	48
<b>8</b>	<b>SECURITY AUDITS .....</b>	<b>48</b>
8.1	Internal Security Audits .....	48
8.2	Software Application Audits .....	49
8.3	Third Party Audits .....	50
<b>9</b>	<b>FRAUD DETECTION .....</b>	<b>50</b>
9.1	Fraud Detection on Internally Posted Jobs .....	51
9.1.1	Verifying Employer Identity .....	51



9.1.2	Federal Employer ID Number Verification .....	52
9.1.3	Text Watch Alerts .....	52
9.1.4	Suspicious Employer Reports.....	53
9.1.5	Suspicious Employer System Alerts .....	53
9.2	<b>Fraud Detection on External Jobs .....</b>	<b>53</b>
9.3	<b>Other Items that Help Mitigate Fraud .....</b>	<b>54</b>
9.3.1	Warning Messages.....	54
9.3.2	Hiding the Individual's Email Address.....	54
9.3.3	Notifying Potential Victims .....	54
10	<b>SECURITY RESPONSE PROCEDURES .....</b>	<b>54</b>
11	<b>ROLES AND RESPONSIBILITIES .....</b>	<b>57</b>
	<b>APPENDIX A – GLOSSARY AND DEFINITIONS.....</b>	<b>58</b>
	<b>APPENDIX B – SECURITY CONTROLS .....</b>	<b>61</b>
	<b>APPENDIX C – SECURITY GUIDELINES AND STANDARDS .....</b>	<b>68</b>
C.1	National Institute of Standards and Technology (NIST) Special Publication (SP) and Guidelines .....	68
C.2	Federal Information Processing Standards Publications (FIPS) .....	69
C.3	Federal Laws.....	69
	<b>APPENDIX D – SECURITY STANDARDS AND PROCEDURES .....</b>	<b>70</b>
D.1	Risk Assessment – Standards and Procedures .....	70
D.2	System Operations – Standards and Procedures .....	72
D.3	System Operations – Prohibited Activities .....	83
D.4	Physical and Environmental Security – Standards and Procedures.....	85
D.5	Application Security – Standards and Procedures .....	87
D.6	Access Controls – Standards and Procedures .....	89
D.7	Acceptable Use – Standards and Procedures.....	91
D.8	Acceptable Use – Prohibited Activities.....	93
D.9	Data/Equipment Handling and Disposal – Standards and Procedures.....	94
D.10	Security Incident Response – Standards and Procedures .....	94

D.11 Personnel Security – Standards and Procedures .....	96
D.12 Training and Awareness – Standards and Procedures.....	97
D.13 Vendor Management and Third Party Access – Standards and Procedures .....	98
D.14 Disaster Recovery – Standards and Procedures .....	99
D.15 Disaster Recovery – Assumptions .....	100
D.16 Security Review and Audit – Standards and Procedures .....	101

Draft

## Introduction

Geographic Solutions' comprehensive security program is an integral part of our product and environment design and development lifecycle. Geographic Solutions adheres to a detailed risk assessment process and defense-in-depth to properly define requirements and design appropriate security solutions. Geographic Solutions focuses on ensuring data confidentiality, availability, and integrity to ensure the satisfaction of all client security policies. Geographic Solutions' security architecture leverages an integrated set of enterprise services so the Indiana Department of Workforce Development (DWD) can focus on business goals rather than security implementation.

Geographic Solutions understands the importance of information security. Security threats can come from many different sources, such as the Internet or from inside the network. Geographic Solutions has developed System Security Plans (SSP) for several state and local systems.

# 1 Security Plan Outline

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 2 Security Architecture

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

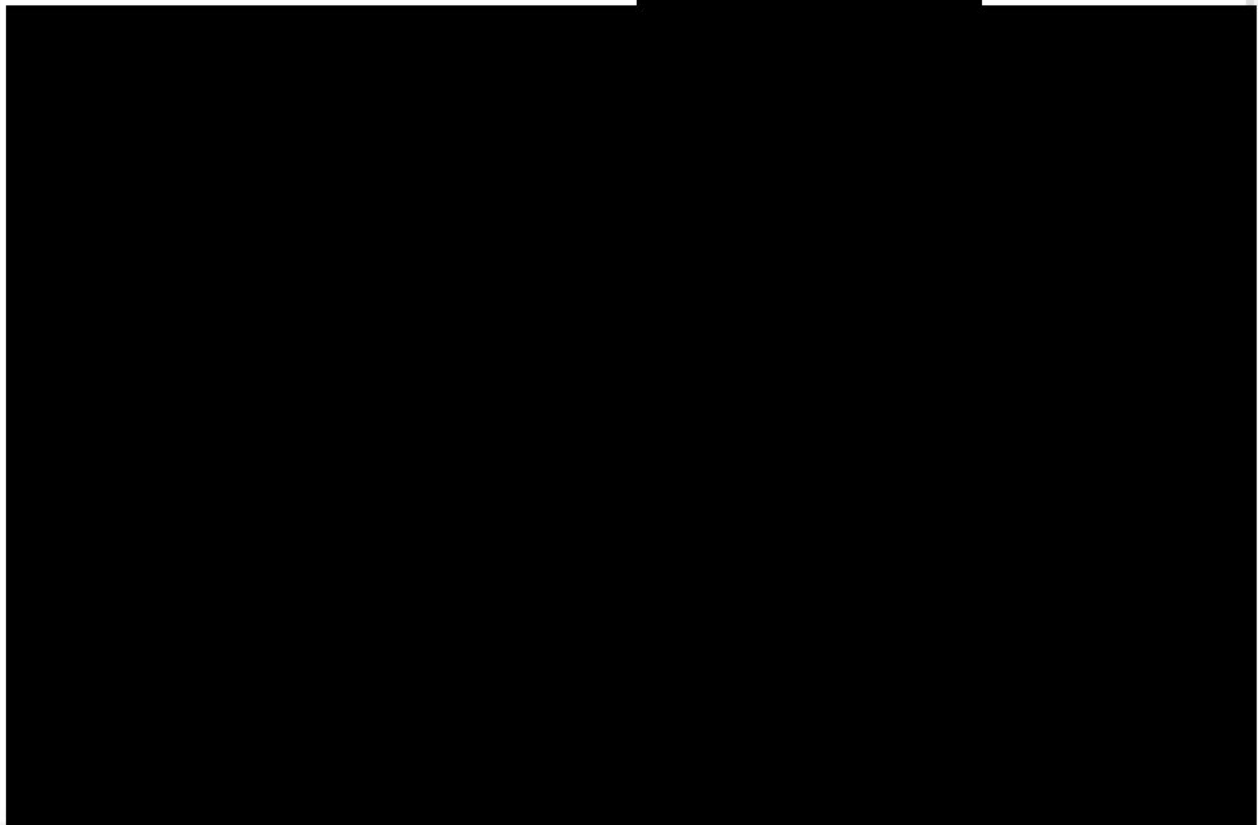
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



*Geographic Solutions Virtual OneStop Security Architecture*

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 3 Multi Layered Security Defenses

[REDACTED]

[REDACTED]

[REDACTED]







	<div></div> <div></div>	<div></div> <div></div> <div></div>
	<div></div>	<div></div>
<div></div> <div></div>	<div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>
	<div></div> <div></div>	<div></div> <div></div>
	<div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div> <div></div>
	<div></div> <div></div>	<div></div> <div></div> <div></div>
	<div></div>	<div></div> <div></div>
<div></div> <div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>
	<div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div>

[Redacted text block]

## 4 Infrastructure Protection

[Redacted text block]

### 4.1 Security Information and Event Management (SIEM)

[Redacted text block]



- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 4.2 Centralized Security Management

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 4.3 Network Perimeter Protection and Intrusion Detection

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]



## 4.3.2 Intrusion Protection

[REDACTED]

### 4.3.2.1 Network Perimeter Intrusion Protection

[REDACTED]

### 4.3.2.2 Active Malware Detection

[REDACTED]

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[REDACTED]

[REDACTED]

[REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]

[REDACTED]

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

## 4.4 Endpoint and Server Protection

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

## 4.5 Internal Network Protection

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 4.6 Physical Security of Geographic Solutions Infrastructure

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 4.6.1 Access Controls and Equipment

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 4.6.2 Visitor and Authorized Personnel Access Control

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 4.6.3 Workstation & Internal Network Protection

[REDACTED]

[REDACTED]

[REDACTED]

## 5 Data Security - Securing Client Information

[REDACTED]

### 5.1 Protecting Data at Rest and in Use

[REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 5.2 Protecting Data in Transit

[REDACTED]

[REDACTED]

[REDACTED]

## 5.3 Web Services Authentication and Encryption

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	■	■	■	■	■	■	■	
[REDACTED]			■		■	■		
[REDACTED]							■	■
[REDACTED]	■	■	■		■	■		
[REDACTED]	■	■	■		■	■		

[REDACTED]

## 5.4 Database Access Protection

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 5.5 Data Encryption

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 5.5.1 Hardware Encryption

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 5.5.2 Software Encryption

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 5.5.3 FTP Encryption

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

### 5.5.4 Backup Encryption

## 6 Application Protection

### 6.1 Architecture and Code Design Standards and Best Practices

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

### 6.1.1 SANS Top 25 Most Dangerous Programming Errors

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]



[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

## 6.2 Strong Application Access Controls

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

### 6.2.1 Application User Authentication

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

## 6.2.2 Single Sign On

[REDACTED]

[REDACTED]

[REDACTED]

## 6.2.3 Maintaining Credential Security

[REDACTED]

### 6.2.3.1 Username and Password Complexity and Content

[REDACTED]

### 6.2.3.2 Password Expiration

[REDACTED]

### 6.2.3.3 Password Changes and Automated Retrieval

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 6.2.3.4 Session Timeout

[REDACTED]

### 6.2.3.5 Disable an Account for Unsuccessful Password Entry

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 6.2.3.6 Terminating Users

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

#### 6.2.3.7 Customized Login Messages

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 6.2.4 Network User Authentication

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

## 6.2.5 Strong Data Access Controls

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

### 6.3 Full Role-Based Security Model

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_





[illegible]

[REDACTED]

### 6.4.1 Audit Logs

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 6.4.2 Transaction Logging

[REDACTED]

- [REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

## 7 Organizational Protection

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

### 7.1 Strict Security Policies and Procedures

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- CONFIDENTIAL  
Appendix I – 44

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

### 7.1.1 Geographic Solutions Password Policy

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 7.1.2 Sanitation and Destruction of Sensitive Information

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

## 7.2 Background Screening

[REDACTED]

[REDACTED]

## 7.3 Security Training and Education

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

## 7.4 Risk Management

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 8 Security Audits

[REDACTED]

[REDACTED]

### 8.1 Internal Security Audits

[REDACTED]

[REDACTED]

[REDACTED] se

audits include threat and vulnerability assessments (automated network and agent scanning based

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 8.2 Software Application Audits

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

### 8.3 Third Party Audits

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 9 Fraud Detection

[REDACTED]

## 9.1 Fraud Detection on Internally Posted Jobs

### 9.1.1 Verifying Employer Identity

[REDACTED] all job orders prior to posting. This is a less commonly used option due to the staff time involved.

## 9.1.2 Federal Employer ID Number Verification

[REDACTED]

[REDACTED]

[REDACTED]

## 9.1.3 Text Watch Alerts

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Message folder in the Virtual OneStop

Message Center and blocks any other associated email.

## 9.1.4 Suspicious Employer Reports

[REDACTED]

[REDACTED]

[REDACTED]

## 9.1.5 Suspicious Employer System Alerts

[REDACTED]

## 9.2 Fraud Detection on External Jobs

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

### 9.3 Other Items that Help Mitigate Fraud

[REDACTED]

#### 9.3.1 Warning Messages

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 9.3.2 Hiding the Individual's Email Address

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 9.3.3 Notifying Potential Victims

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 10 Security Response Procedures

[REDACTED]

[REDACTED]ity



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]


[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

- 
- | Row | Bar Length (approx. % of total width) |
|-----|---------------------------------------|
| 1   | 95                                    |
| 2   | 85                                    |
| 3   | 98                                    |
| 4   | 45                                    |
| 5   | 88                                    |
| 6   | 99                                    |
| 7   | 65                                    |
| 8   | 98                                    |
| 9   | 85                                    |
| 10  | 92                                    |
| 11  | 42                                    |
| 12  | 95                                    |

[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

















[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Draft



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## C.2 Federal Information Processing Standards Publications (FIPS)

- [REDACTED]
- [REDACTED]
- [REDACTED]

## C.3 Federal Laws

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

## Appendix D – Security Standards and Procedures

### D.1 Risk Assessment – Standards and Procedures

[REDACTED]

[REDACTED]

- I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
- I [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
- I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
  - I [REDACTED]
- I [REDACTED]
  - [REDACTED]





## D.2 System Operations – Standards and Procedures

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]









[REDACTED]

[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]







[REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



## D.3 System Operations – Prohibited Activities

[REDACTED]

[REDACTED]

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



## D.4 Physical and Environmental Security – Standards and Procedures

[REDACTED]

[REDACTED]

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





## D.5 Application Security – Standards and Procedures

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
  - [REDACTED]
- [REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]



- | [REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]





\_\_\_\_\_

\_\_\_\_\_

- [illegible]

## D.9 Data/Equipment Handling and Disposal – Standards and Procedures

[REDACTED]

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

## D.10 Security Incident Response – Standards and Procedures

[REDACTED]

[REDACTED]

- I [REDACTED]
- I [REDACTED]

[REDACTED]

[REDACTED]





- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
- [REDACTED]
- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
- [REDACTED]
  - [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

## D.11 Personnel Security – Standards and Procedures

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
  - [REDACTED]
    - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

- [REDACTED]  
 ■ [REDACTED]  
 ■ [REDACTED]  
 ■ [REDACTED]  
 ■ [REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]

## D.13 Vendor Management and Third Party Access – Standards and Procedures

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]
- [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

## D.14 Disaster Recovery – Standards and Procedures

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

-

1 [REDACTED]  
[REDACTED]

2 [REDACTED]  
[REDACTED]

3 [REDACTED]

4 [REDACTED]  
[REDACTED]  
[REDACTED]

5 [REDACTED]  
[REDACTED]

6 [REDACTED]  
[REDACTED]

7 [REDACTED]  
[REDACTED]  
[REDACTED]

8 [REDACTED]  
[REDACTED]  
[REDACTED]

9 [REDACTED]  
[REDACTED]

10 [REDACTED]  
[REDACTED]  
[REDACTED]