

## InnoCentive Security Procedure

<b>Effective Date:</b>	14-JUN-2005
<b>Supersedes:</b>	None
<b>Associated Documents:</b>	InnoCentive Backup and Restoration Procedure InnoCentive System Inventory InnoCentive Application Installation and Verification Instructions (IVI) SQL Server Installation Instructions InnoCentive Procedure for Change Control Preparation, Review, and Approval
<b>Approved by:</b>	CEO
<b>Signature:</b>	
<b>Date:</b>	
<b>Approved by:</b>	VP Operations and CFO
<b>Signature:</b>	
<b>Date:</b>	

### Revision History:

Version	Date	Editor	Comments
1.0	14-JUN-2005	Safis Solutions	New Document

## Table of Contents

<b>1. Introduction.....</b>	<b>3</b>
1.1 Purpose.....	3
1.2 Scope.....	3
1.2.1 In-Scope .....	3
1.2.2 Out of Scope.....	3
<b>2. Physical Security.....</b>	<b>3</b>
2.1 Physical Security Controls.....	3
2.2 Physical Security Access Request Process .....	3
2.2.1 Temporary Physical Security Access .....	4
2.2.2 Removing Physical Security Access .....	4
<b>3. Logical Security.....</b>	<b>4</b>
3.1 Logical Security Controls .....	4
3.1.1 User IDs and Passwords.....	5
3.1.2 System Clock.....	5
3.1.3 Automatic System Time-out .....	5
3.1.4 Virus Protection .....	5
3.2 Logical Security Account Access Request Process .....	5
3.2.1 Temporary Logical Security Access .....	7
3.2.2 Modifying Logical Security Access .....	7
3.2.3 Deactivating Logical Security Access .....	7
3.3 Automatic Account Deactivation .....	7
3.4 System-Specific Logical Security Access Levels .....	8
3.4.1 Andover .....	8
3.4.2 Development Server.....	8
3.4.3 InnoCentive.com.....	8
3.4.4 Challenge Manager .....	8
3.4.5 CVS .....	9
3.4.6 MySQL.....	9
<b>4. Security Risks and Countermeasures .....</b>	<b>9</b>
4.1 Andover.....	9
4.2 Innocentive.com.....	10
4.3 Challenge Manager .....	10
4.4 Production Servers/Sterling Data Center .....	11
<b>Appendix A: Account Access Request Form.....</b>	<b>12</b>
<b>Appendix B: Physical Access Request Form.....</b>	<b>14</b>

# 1. Introduction

## 1.1 Purpose

The purpose of this document is to define the physical and logical security controls for InnoCentive systems.

## 1.2 Scope

### 1.2.1 In-Scope

The systems located at Verio and Andover are included in the scope of this Security Plan.

### 1.2.2 Out of Scope

The systems owned by vendors are not in the scope of this Security Plan. The *InnoCentive Vendor Assessment and Management Procedure* states that vendors shall have their own security procedures in place and documented. These documents shall be made available to InnoCentive personnel during vendor assessments.

# 2. Physical Security

## 2.1 Physical Security Controls

The InnoCentive Andover offices feature the following physical security controls:

- Key fob access to enter office suite and server room
- Adequate fire protection in the InnoCentive facility and server room
- Server room is temperature and humidity controlled
- Development environment uses Uninterrupted Power Supply (UPS) as a backup power source
- Locked cabinet for Disaster Recovery Plan
- Fire-proof safe for backup media

## 2.2 Physical Security Access Request Process

To gain access to the InnoCentive facility, the locked server room, or any other secure area within the InnoCentive facility, do the following:

- Complete an *InnoCentive Physical Access Request Form* (found in Appendix B of this document).
- Submit the form to the system custodian for approval.

- Once approved, an InnoCentive representative adds the name and type of access granted to the access roster for the facility and/or area to which access is being granted.
- The InnoCentive representative provides the appropriate key fob to the requester.

### **2.2.1 Temporary Physical Security Access**

Temporary physical security access for contractors is established following the process listed in *Section 2.2 Physical Security Access Request Process*. The removal of temporary physical security accounts is managed following the process listed in *Section 2.2.2 Removing Physical Security Access*.

### **2.2.2 Removing Physical Security Access**

The system custodian, in concert with InnoCentive, removes physical security access in the following circumstances:

- Temporary access is no longer needed
- An employee leaves the company

Once the access is removed, the InnoCentive representative updates the access roster for the facility and/or area to which access is being removed to reflect the access change. The representative recovers the key fob from the employee.

## **3. Logical Security**

### **3.1 Logical Security Controls**

The systems and hardware located in the Andover office include the following logical security controls:

- Unique user ID and password to access the domain
- Restricted access to the system clock from a workstation or PC
- Automatic system time-out after a period of inactivity
- Deactivation of a user ID after three unsuccessful login attempts
- Adequate virus protection
- Secure Sockets Layer (SSL) protocol for internet message transmission security

The systems and hardware for the production servers will include the following logical security controls:

- Remote login of root accounts not allowed
- Individual user level accounts will be created for remote login

### 3.1.1 User IDs and Passwords

User IDs are unique and are a minimum of 8 characters. Domain security policies are implemented that require complex, alphanumeric passwords that expire every 60 days. Passwords must be at least 7 characters in length. The last 10 passwords are remembered by the system and cannot be reused.

### 3.1.2 System Clock

System clock may not be updated. This privilege is controlled by a Windows domain security policy.

### 3.1.3 Automatic System Time-out

The automatic system time-out is 15 minutes.

### 3.1.4 Virus Protection

InnoCentive uses Symantec Corporate Antivirus product for virus protection. Virus protection patches are automatically downloaded from the Symantec server. These patches are immediately applied.

## 3.2 Logical Security Account Access Request Process

Site	Process
Andover	<ul style="list-style-type: none"> <li>• User completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>• User submits the form to the system custodian for approval.</li> <li>• Corporate IT creates the account and verbally communicates the unique user ID and password to the requester.</li> <li>• Corporate IT returns form to system custodian for storage.</li> </ul>
innocentive.com	<ul style="list-style-type: none"> <li>• Admins and SciOps accounts:               <ul style="list-style-type: none"> <li>○ The product manager completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>○ The product manager submits the form to the system custodian for approval.</li> <li>○ The product manager creates the new account and verbally communicates the unique user ID and password to the requester.</li> <li>○ The product manager returns form to system custodian for storage.</li> </ul> </li> <li>• User accounts:               <ul style="list-style-type: none"> <li>○ The user follows online registration process.</li> </ul> </li> </ul>
Challenge Manager	<ul style="list-style-type: none"> <li>• Admins and SciOps accounts:               <ul style="list-style-type: none"> <li>○ The product manager completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>○ The product manager submits the form to the system custodian for approval.</li> <li>○ The product manager creates the new account and verbally communicates the unique user ID and password to the requester.</li> <li>○ The product manager returns form to system custodian for storage.</li> </ul> </li> <li>• Champion accounts:</li> </ul>

Site	Process
	<ul style="list-style-type: none"> <li>○ The product manager completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>○ The product manager submits the form to the system custodian for approval.</li> <li>○ The product manager creates the account and verbally communicates the password to the requester. (user id is the email address)</li> <li>○ The product manager returns form to system custodian for storage.</li> <li>● Seeker Manager and Seeker User accounts:               <ul style="list-style-type: none"> <li>○ The user follows online registration process.</li> </ul> </li> </ul>
Production servers	<ul style="list-style-type: none"> <li>● All accounts:               <ul style="list-style-type: none"> <li>○ The product manager or vendor project manager completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>○ The product manager or vendor project manager submits the form to the system custodian for approval.</li> <li>○ The product manager or vendor project manager forwards information to Verio via <a href="http://powerportal.verio.com">http://powerportal.verio.com</a> to handle the request.</li> <li>○ The product manager or vendor project manager verbally communicates the unique user ID and password combination to the requester.</li> <li>○ The product manager or vendor project manager returns the form to system custodian for storage.</li> </ul> </li> </ul>
Verio Power Portal	<p>The Verio Power Portal manages technical and billing issues for Verio servers. It provides access to trouble tickets, account information, and remote backup and restoration management.</p> <ul style="list-style-type: none"> <li>● Only Verio, the InnoCentive system custodian, the InnoCentive product manager and the IT vendor project manager require access to the portal.               <ul style="list-style-type: none"> <li>○ The InnoCentive product manager completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>○ The InnoCentive product manager submits the form to the InnoCentive system custodian for approval.</li> <li>○ The InnoCentive product manager forwards information to Verio via <a href="http://powerportal.verio.com">http://powerportal.verio.com</a> to handle the request.</li> <li>○ Verio communicates the unique user ID and password combination to the requester and notifies the InnoCentive product manager.</li> <li>○ The InnoCentive product manager returns the form to InnoCentive system custodian for storage.</li> </ul> </li> </ul>
Verio Managed Services Portal	<p>The Managed Services Customer Portal is a sub-portal within the Verio Power Portal. It offers secure real-time access to reports, charts and utilities, enabling staff to quickly review logs, submit policy changes and enter service requests.</p> <ul style="list-style-type: none"> <li>● Only Verio, the InnoCentive system custodian, the InnoCentive product manager and the IT vendor project manager require access to the portal.               <ul style="list-style-type: none"> <li>○ The InnoCentive product manager completes an <i>InnoCentive Account Access Request Form</i>.</li> <li>○ The InnoCentive product manager submits the form to the InnoCentive system custodian for approval.</li> <li>○ The InnoCentive product manager forwards information to Verio via <a href="https://iss.powerportal.verio.net">https://iss.powerportal.verio.net</a> to handle the request.</li> <li>○ Verio communicates the unique user ID and password combination to the requester and notifies the InnoCentive product manager.</li> <li>○ The InnoCentive product manager returns the form to InnoCentive system custodian for storage.</li> </ul> </li> </ul>

Site	Process
	storage.

### 3.2.1 Temporary Logical Security Access

Temporary logical security access to an InnoCentive system for contractors is established following the process listed in *Section 3.2 Logical Security Account Access Request Process*. The deactivation of temporary logical security accounts is managed following the process listed in *Section 3.2.3 Deactivating Logical Security Access*.

### 3.2.2 Modifying Logical Security Access

If modifications need to be made to a user account:

- Complete a new *InnoCentive Account Access Request Form*.
- Submit the form to the system custodian for approval.
- Once approved, the system custodian directs that the appropriate security group is modified.

### 3.2.3 Deactivating Logical Security Access

The system custodian deactivates user accounts in the following circumstances:

- Temporary access to a system is no longer needed
- An employee leaves the company

## 3.3 Automatic Account Deactivation

Access is not automatically denied after unsuccessful attempts to access InnoCentive or Challenge Manager.

Management has evaluated risk and cost benefit of an account lock-out policy and has decided to allow an unlimited number of attempts to log in to either system. Challenge Manager is IP restricted.

The following table shows the current policy for account lock-out:

Lock Policy	Server Acct	Innocentive.com	Challenge Manager
N	Nobody	Solver	---
N	Nobody	Sciops	Sciop
N	Nobody	Admin	Admin
N	Nobody	Seekers	-----
N	Nobody	"	Champion
N	Nobody	"	Manager
N	Nobody	"	User

Lock Policy	Server Acct	Innocentive.com	Challenge Manager
N	root		
N	root2		
N	mysql		

## 3.4 System-Specific Logical Security Access Levels

### 3.4.1 Andover

Access Level	Access Level Description
Administrators	<ul style="list-style-type: none"> <li>Have complete and unrestricted access to the computer/domain.</li> </ul>
Domain Admins	<ul style="list-style-type: none"> <li>Administrators of the domain.</li> </ul>
Domain Power Users	<ul style="list-style-type: none"> <li>Perform basic administrative tasks.</li> <li>Cannot log on to the server locally.</li> </ul>
Domain Users	<ul style="list-style-type: none"> <li>Users of the domain.</li> </ul>
Remote Web Workplace Users	<ul style="list-style-type: none"> <li>Remote users of the domain.</li> <li>Can access the Remote Web Workplace from the Internet.</li> </ul>

### 3.4.2 Development Server

Access Level	Access Level Description
Administrators	<ul style="list-style-type: none"> <li>Have complete and unrestricted access to the computer/system.</li> </ul>
Users	<ul style="list-style-type: none"> <li>Users of the system.</li> </ul>
CVS	<ul style="list-style-type: none"> <li>Group that allows access to CVS.</li> </ul>
Scarab	<ul style="list-style-type: none"> <li>Group that allows access to Scarab.</li> </ul>
MySQL	<ul style="list-style-type: none"> <li>MySQL user.</li> </ul>

### 3.4.3 InnoCentive.com

Access Level	Access Level Description
Administrators	<ul style="list-style-type: none"> <li>Have complete and unrestricted access to the application.</li> </ul>
SciOps	<ul style="list-style-type: none"> <li>Have access to all challenges and submissions.</li> </ul>
Solvers	<ul style="list-style-type: none"> <li>Have access to challenges and their own submissions.</li> </ul>
Seekers	<ul style="list-style-type: none"> <li>Have access only to their challenges.</li> </ul>
Guests	<ul style="list-style-type: none"> <li>Have access to public areas of application.</li> </ul>

### 3.4.4 Challenge Manager

Access Level	Access Level Description
Administrators	<ul style="list-style-type: none"> <li>Have complete and unrestricted access to the application.</li> </ul>
SciOps/GAMs	<ul style="list-style-type: none"> <li>Have access to challenges and submissions.</li> </ul>
Seeker Champions	<ul style="list-style-type: none"> <li>Have access to all challenges for their organization.</li> </ul>

Access Level	Access Level Description
Seeker Managers	<ul style="list-style-type: none"> <li>Have read-only access to all challenges for their organization.</li> <li>Have access to their challenges.</li> </ul>
Seeker Users	<ul style="list-style-type: none"> <li>Have access to assigned challenges.</li> </ul>

### 3.4.5 CVS

Access Level	Access Level Description
Administrators	<ul style="list-style-type: none"> <li>Create and deactivate accounts.</li> <li>Restrict directory access.</li> <li>Create, modify, and delete directories.</li> </ul>
Users	<ul style="list-style-type: none"> <li>Check documents in and out based on directories they can access.</li> </ul>

### 3.4.6 MySQL

Access Level	Access Level Description
Administrators	<ul style="list-style-type: none"> <li>Maintain the database.</li> </ul>
CRUD	<ul style="list-style-type: none"> <li>Create, read, update, and delete capability.</li> </ul>

## 4. Security Risks and Countermeasures

### 4.1 Andover

Risk	Potential Harm	Countermeasure(s)
Unauthorized access to the InnoCentive domain.	Unauthorized user could manipulate files and/or data.	<ul style="list-style-type: none"> <li>Users are assigned appropriate levels of access.</li> <li>Access is deactivated for former employees.</li> <li>A firewall is in place to prevent unauthorized access.</li> <li>Each system requires unique user ID and password combination to gain access that is assigned by the system administrator.</li> <li>User IDs are deactivated after three unsuccessful login attempts.</li> </ul>
Incorrect security access assigned to a user.	User could gain access to confidential information and/or be able to manipulate files and data that he or she should not be able to access.	<ul style="list-style-type: none"> <li>Access rosters are reviewed annually.</li> </ul>
User could manipulate the system clock.	Audit trail data integrity could be compromised.	<ul style="list-style-type: none"> <li>Access to the system clock is restricted.</li> <li>This privilege is controlled by a Windows domain security policy.</li> </ul>

Risk	Potential Harm	Countermeasure(s)
A user could gain access to a system using another user's unattended PC/workstation.	User could gain access to and/or manipulate files and/or data.	<ul style="list-style-type: none"> <li>The Windows operating system is configured to automatically time-out after 15 minutes of inactivity.</li> </ul>
The Andover office could be infected with a virus, Trojan horse, worm, etc.	System files and data could be lost or become corrupt.	<ul style="list-style-type: none"> <li>Virus protection is installed on the Andover servers, PCs, and workstations.</li> <li>A firewall is in place to prevent unexpected attacks on the Andover servers.</li> </ul>

## 4.2 Innocentive.com

Risk	Potential Harm	Countermeasure(s)
Unauthorized access to the InnoCentive.com application.	Unauthorized user could manipulate files and/or data.	<ul style="list-style-type: none"> <li>Users are assigned appropriate levels of access.</li> <li>Access is deactivated for former employees.</li> <li>A firewall is in place to prevent unauthorized access.</li> <li>Each system requires unique user ID and password combination to gain access.</li> </ul>
Incorrect security access assigned to a user.	User could gain access to confidential information and/or be able to manipulate files and data that he or she should not be able to access.	<ul style="list-style-type: none"> <li>Access rosters are reviewed annually.</li> </ul>
User could manipulate the system clock.	Audit trail data integrity could be compromised.	<ul style="list-style-type: none"> <li>Access to the system clock is restricted.</li> </ul>
A user could gain access to a system using another user's unattended PC/workstation.	User could gain access to and/or manipulate files and/or data.	<ul style="list-style-type: none"> <li>The website is configured to automatically time-out after 60 minutes of inactivity.</li> </ul>

## 4.3 Challenge Manager

Risk	Potential Harm	Countermeasure(s)
Unauthorized access to the Challenge Manager application.	Unauthorized user could manipulate files and/or data.	<ul style="list-style-type: none"> <li>Users are assigned appropriate levels of access.</li> <li>Access is deactivated for former employees.</li> <li>A firewall is in place to prevent unauthorized access.</li> <li>Each system requires unique user ID and password combination to gain access.</li> <li>Access is restricted by IP address.</li> <li>Each organization's data is encrypted with a unique key.</li> </ul>

Risk	Potential Harm	Countermeasure(s)
Incorrect security access assigned to a user.	User could gain access to confidential information and/or be able to manipulate files and data that he or she should not be able to access.	<ul style="list-style-type: none"> <li>Access rosters are reviewed annually.</li> </ul>
User could manipulate the system clock.	Audit trail data integrity could be compromised.	<ul style="list-style-type: none"> <li>Access to the system clock is restricted.</li> </ul>
A user could gain access to a system using another user's unattended PC/workstation.	User could gain access to and/or manipulate files and/or data.	<ul style="list-style-type: none"> <li>The website is configured to automatically time-out after 60 minutes of inactivity.</li> </ul>

#### 4.4 Production Servers/Sterling Data Center

Risk	Potential Harm	Countermeasure(s)
Unauthorized access to the production servers.	Unauthorized user could manipulate files and/or data.	<ul style="list-style-type: none"> <li>Users are assigned appropriate levels of access.</li> <li>Access is deactivated for former employees.</li> <li>A firewall is in place to prevent unauthorized access.</li> <li>Each system requires unique user ID and password combination to gain access.</li> <li>Access is restricted by IP address.</li> <li>An intrusion prevention system (Proventia G series) is in place to monitor and block suspicious traffic.</li> </ul>
Incorrect security access assigned to a user.	User could gain access to confidential information and/or be able to manipulate files and data that he or she should not be able to access.	<ul style="list-style-type: none"> <li>Access rosters are reviewed annually.</li> </ul>
User could manipulate the system clock.	Audit trail data integrity could be compromised.	<ul style="list-style-type: none"> <li>Access to the system clock is restricted.</li> </ul>
A user could gain access to a system using another user's unattended PC/workstation.	User could gain access to and/or manipulate files and/or data.	<ul style="list-style-type: none"> <li>The servers are configured to automatically time-out after 2 hours of inactivity.</li> </ul>

## **Appendix A: Account Access Request Form**

## InnoCentive Account Access Request Form

<b>Date Requested:</b>	<b>Date Needed:</b>	<b>Employee</b> <input type="checkbox"/> <b>Contractor</b> <input type="checkbox"/>
------------------------	---------------------	--

**Type of Request:**

**New** 
                         
 **Change** 
                         
 **Remove**

**If removal, please explain:**

**Requester Information:**

Employee ID:		Account Name (if existing):	
Full Name:		Email Address:	
Home Address:		City, State, Zip:	
Home/Cell Phone:	(    )	Work Phone:	(    )

**Access Needed:**

Andover		Development Server		Innocentive.com	
Administrator	<input type="checkbox"/>	Administrator	<input type="checkbox"/>	Administrator	<input type="checkbox"/>
Domain Admin	<input type="checkbox"/>	User	<input type="checkbox"/>	SciOps	<input type="checkbox"/>
Domain Power User	<input type="checkbox"/>	CVS	<input type="checkbox"/>	Solver	<input type="checkbox"/>
Domain User	<input type="checkbox"/>	Scarab	<input type="checkbox"/>	Seeker	<input type="checkbox"/>
Remote Web Workplace User	<input type="checkbox"/>	MySQL	<input type="checkbox"/>		
Challenge Manager		CVS*		Production Server	
Administrator	<input type="checkbox"/>	Administrator	<input type="checkbox"/>	super user	<input type="checkbox"/>
SciOps/GAMs	<input type="checkbox"/>	User	<input type="checkbox"/>	user	<input type="checkbox"/>
Seeker Champion	<input type="checkbox"/>	MySQL			
Seeker Manager	<input type="checkbox"/>	Administrator	<input type="checkbox"/>		
Seeker User	<input type="checkbox"/>	CRUD	<input type="checkbox"/>		

\*Note: Access is restricted to cvs only. Ensure that no super user login access is granted.

**Approval and Signature**

Requester Signature:	Date:
----------------------	-------

Supervisor Approval:	Date:
----------------------	-------

System Custodian Approval:	Date:
----------------------------	-------

## **Appendix B: Physical Access Request Form**

## InnoCentive Physical Access Request Form

<b>Date Requested:</b>	<b>Date Needed:</b>	<b>Employee</b> <input type="checkbox"/>	
		<b>Contractor</b> <input type="checkbox"/>	
<b>Type of Request:</b>			
<b>New</b> <input type="checkbox"/>	<b>Change</b> <input type="checkbox"/>	<b>Remove</b> <input type="checkbox"/>	
<b>If removal, please explain:</b>			
<b>Requester Information:</b>			
Employee ID:		Account Name (if applicable):	
Full Name:		Email Address:	
Home Address:		City, State, Zip:	
Home/Cell Phone:	(    )	Work Phone:	(    )
<b>Access Needed:</b>			
Key Fob to Office	<input type="checkbox"/>	Number/Details:	
Key Fob to Server Room	<input type="checkbox"/>	Number/Details:	
Locked Cabinet	<input type="checkbox"/>	Number/Details:	
Fire-proof safe	<input type="checkbox"/>	Number/Details:	
<b>Approval and Signature</b>			
Requester Signature:		Date:	
Supervisor Approval:		Date:	
System Custodian Approval:		Date:	

