

VENDOR SECURITY QUESTIONNAIRE

On Site Audit Date :
Auditor Name:
Auditor Contact Number

Controls	Questions	Yes	No	NA	Documentation Provided/Comments
Physical Security					
,	Is the office in a single tenant building?				
	Are the entrances locked?				
	Do the entrances have key access controls?				
	Do the entrances have badge access controls?				
	Are there security guards on site?				
	Does the vendor have a burglar alarm system?				
	Are there security cameras for the facility?				
	If so, are the recordings saved?				
	Is there a backup generator in the event of				
	power loss?				
Change Control	Is there a fire suppression system?				
Change Control	When regulatory or process changes are made				
	When regulatory or process changes are made by Safeguard, does the vendor communicate				
	those changes to all their employees?				
Encryption	those changes to all their employees:				
Encryption	Do the vendor's systems have any special				
	encryption technology in place and utilized?				
Data Integrity	eneryption teermology in place and atmized.			L	
Data intogrity	Does the vendor have sufficient checks and				
	balances in place to ensure data integrity?				
Logical Access	p				
J	Does the vendor ensure that access is revoked				
	to employees that have been let go?				
Communications ar	nd Connectivity			_	
	What type of internet connectivity does the vendor have?				
	Does the vendor take reasonable precautions to				
	insure that confidential information is not				
	transferred by email or other chat?				
Incident Response					
	Do procedures exist to deal with the				
	identification and detection of security breaches?				
DR/BCP			-		
	Does the vendor have a formal documented				
	recovery plan for the resumption of business?				
Backup and Offsite	_				
	Does the vendor maintain backup data and				
	records for the work they have been assigned?				
	If so, where and in what form, do they exist?				

Media and Vital Records



VENDOR SECURITY QUESTIONNAIRE

On Site Audit Date :	
Auditor Name:	
Auditor Contact Number: _	

Controls	Questions	Yes	No	NA	Documentation Provided/Comments
	Does the Vendor safely and securely dispose of confidential information and information systems? Does the vendor possess paper shredders for				
	disposing of confidential documents?				
Third Party Relatio	nships Do any third party relationships exist? *See definitions below.				
Regulatory Require					
	Does the vendor and their staff adhere to all compliance regulations dealing with their business?				
Training					
	Are vendor's employees trained in how to handle and report security breaches?				
Operations				Ι	
	Does the vendor have documented standard operating procedures for its business functions?				
Asset managemen	t				
	Are there procedures in place for the disposal or reuse of technology assets and software?				
	Please describe these procedures. How many years of Safeguard data do you keep?				
Desktop	Tiow many years or saregular data do you keep:				
Безкіор	Does the Vendor store any Safeguard Confidential data on their laptops or PC's?				
Application	confidential data on their laptops of 1 c s:				
	Does the Vendor host their own applications or websites, or use another vendors websites, other than Safeguard Properties, to help manage their business workflow?				
	If so, please provide their names or web			ļ	
System Developme	ent	1	1	ı	
	Does the vendor perform or have performed for them, software development?				
Customer Contact				l	
	Are customer service agents trained to safeguard the information they have access to from social engineering tactics?				
	If so, please attach the procedures / awareness				

Page 2 of 2

^{*} A third party organization that routinely receive, send, transmit, store, control, or process Safeguard information that is Confidential or Highly Confidential, or that provide technology and/or non-technology related services that require or include handling such information. The Service Provider should have a process to review all dependent Third Party Service Providers' (i.e., subcontractors) security policies and procedures to ensure that appropriate security language is incorporated into all third-party agreements. Service Providers should ensure that affected financial institutions are aware of any outsourcing and that any required due diligence is completed.