Vendor Risk Assessment

DOCUMENT VERSION:

Date Submitted: _____

Date Reviewed w/Edits: _____

Example Only
Not Represented to be
Approved by Regulators

TABLE OF CONTENTS

Important: View this document in "Print Layout" to see checkboxes. View layout can be changed under View menu.

Overview

This document provides Questionnaires to assess the security controls in place at the outside vendor to safeguard MMFG data entrusted to the vendor.

The following information is covered in this document:

- Vendor Pre-Assessment Questionnaire
- Vendor Risk Assessment Questionnaire

Important: View this document in "Print Layout" to see checkboxes. View layout can be changed under View menu.

Vendor Pre-Assessment Questionnaire

This section is for the reference of the Vendor Relation Manager\Project Manager facilitating this assessment. Please use this section to determine the impact of this engagement to the overall security of information.

Important: View this document in "Print Layout" to see checkboxes. View layout can be changed under View menu. Mark boxes by typing an "X" in the appropriate box.

	Name/Date completed
1. **Data Sensitivity:** What is the nature of data that vendor will have access to? (Mark all that apply) No Risk: No data exchanged, no security impact ☐ Low Risk: Only Demographic information and projected financial info ☐ Medium Risk: Only Names, Addresses and Phone Numbers ☐ High Risk: Non-public Private Information (NPI), for example SSN, medical, financial, proprietary and private information about real individuals	
2. Complete the Vendor Risk Assessment Questionnaire Complete survey, obtaining information from vendor as noted. Please return the completed questionnaire to Information Security consultant assigned to your project. Please make sure the email subject contains the line: Vendor Risk Assessment	

Vendor Risk Assessment Questionnaire

Vendor Name: **Address:**

Vendor Contact Name:

Vendor Contact's Phone Number:

Vendor Contact's Email Address:

Instructions:

- Please complete the following questionnaire.
  - For requests for details/description, please describe in Comments (or "Additional Information and Comments" section at end of questionnaire) or attach documentation with the details.
  - Use N/A for Not Applicable where needed – enter under Comments).
  - Helpful hints:
    - View this document in "Print Layout" to see checkboxes. View layout can be changed under View menu.
    - Mark boxes by typing an "X" in the appropriate box.

Risk Assessment Categories	Yes	No	Comments
Policies and Procedures			
Has the security policy document(s) been published and enforced in your organization?	☐	☐	
Do you have policies and procedures covering the following:			
• HR Practices?	☐	☐	
• Authorized/acceptable use of Networked Services?	☐	☐	
• Use of Corporate Email, intranet and Internet?	☐	☐	
• Password Management?	☐	☐	
• Software/Hardware Acquisition?	☐	☐	
• Change Management?	☐	☐	
• Encryption Policy and Standards?	☐	☐	
• Security related incidence response/handling?	☐	☐	
• Data Handling Policy (to include data use, storage and destruction of sensitive data)?	☐	☐	
• Third Party Access & Remote Access?	☐	☐	
Do you outsource any security management functionality?	☐	☐	
Are policies and procedures updated frequently?	☐	☐	
Is a senior corporate official directly responsible for the implementation of your organizational security policy?	☐	☐	
Are procedures employed to ensure compliance with privacy laws/regulation requirements related to maintaining security, confidentiality and protection of customer data?	☐	☐	
Do you have Information Security staff dedicated to the following:			
• Security Awareness?	☐	☐	
• Policy Enforcement?	☐	☐	
• Risk Evaluation?	☐	☐	
• Risk Mitigation?	☐	☐	

• Regulatory Compliance?	☐	☐	
Are the consequences of non-compliance to the policies clearly documented?	☐	☐	
Patch Management	**Yes**	**No**	**Comments**
Do you apply security patches on a regular basis?	☐	☐	
Do you have an automated patch management solution deployed?	☐	☐	
Do you have vendor agreements in place for timely availability and application of software updates?	☐	☐	
Physical Security	**Yes**	**No**	**Comments**
What kind of perimeter control(s) is applied to data center location?			
• Tokens/Cards?	☐	☐	
• Key Pad Controls?	☐	☐	
• Man Trap?	☐	☐	
• Biometric Controls?	☐	☐	
• Guards?	☐	☐	
Do you monitor/log all access to data center?	☐	☐	
Do you have redundant public utilities connections?	☐	☐	
Do you employ UPS (Uninterrupted Power Supply), Battery Banks, Generators etc?	☐	☐	
Do you employ fire/flood detection and suppression systems?	☐	☐	
Do you monitor and escort visitors through critical parts of your company?	☐	☐	
Do you maintain visitor logs for more than 30 days?	☐	☐	
Information Security Administration	**Yes**	**No**	**Comments**
Can you provide a recent SAS70 report or other industry recognized audit report?	☐	☐	
Do you limit administrator level access on network and systems infrastructure?	☐	☐	
Is your Information Security staff professionally certified (ISC^{2} or SANS)?	☐	☐	
What is the average tenure of your Information Security staff?	☐ 1-3 years ☐ 3-5 years ☐ 5+ years		
Is access to security logs strictly controlled (Firewall logs, etc.)?	☐	☐	
Do you employ version management, build & deploy process?	☐	☐	
Network Infrastructure	**Yes**	**No**	**Comments**
Do you maintain up-to-date network infrastructure and administration procedures?	☐	☐	
Do you have perimeter scanning/monitoring agreements with managed network services providers?	☐	☐	
Are all your routers configured with access control lists to allow only specific traffic to pass through?	☐	☐	
Do you allow access to your routers via its console port only?	☐	☐	
Are all your networking devices at the latest patch level?	☐	☐	
Do you have a procedure to keep track of announcement of vulnerability patches for your networking devices?	☐	☐	
Do you ensure default passwords are changed on networking devices?	☐	☐	
Do you control the change frequency and distribution of admin access to network infrastructure?	☐	☐	
Do you use 802.1x complaint security for your wireless network?	☐	☐	
Do you employ the following intrusion prevention/detection system:			

• HIDS?	☐	☐	
• NIDS?	☐	☐	
• Honey Pots?	☐	☐	
• Rogue device and services detection?	☐	☐	
Remote Access and VPN	**Yes**	**No**	**Comments**
Are there any remote access/remote control methods available to access your network, as follows:			
• Call backs?	☐	☐	
• PKI?	☐	☐	
• RADIUS/TACACS?	☐	☐	
• User ID/Password?	☐	☐	
• Token bases access control?	☐	☐	
• Other? – If yes, what?	☐	☐	
Do you allow supervisory/admin functions to be performed over unencrypted external links?	☐	☐	
Do you collect/review audit log data on remote access?	☐	☐	
Firewall and Intrusion Detection/Prevention	**Yes**	**No**	**Comments**
Do you have a security team that keeps track of all known vulnerabilities?	☐	☐	
Do you have an Intrusion Detection System implemented?	☐	☐	
Do you have an Incident response team?	☐	☐	
Do you employ Firewall server(s) to protect your network?	☐	☐	
Do you have any other applications (e.g. DNS) running on the same Firewall Server?	☐	☐	
Are your Firewall Server's Operating system & software at the latest patch level?	☐	☐	
Do you allow non-standard (>1024) IP ports passing through your Firewall?	☐	☐	
Have you scanned and verified all the allowable services provided by your Firewall server?	☐	☐	
Do you use firewall-reporting tools to analyze your Firewall log?	☐	☐	
Do you have your security policy on your firewall documented and verified?	☐	☐	
Do you protect your internal IP address range(s) (E.g., use NAT/RFC 1918)?	☐	☐	
Mal-ware Controls	**Yes**	**No**	**Comments**
Do you scan all emails for viruses?	☐	☐	
Is there explicit policy requiring anti-virus software on networked computers?	☐	☐	
Do you have centralized administration of virus control, such as distribution of signature updates, reporting, policy enforcement and vendor management?	☐	☐	
Are rules established for scanning outside software?	☐	☐	
Does the virus checking software run in the background with established frequency of scanning etc	☐	☐	
Are end-users prevented from disabling anti-virus software on personal computers?	☐	☐	
Do you allow installation of personal and non-corporate approved software on network computers?	☐	☐	
Disaster Recovery and Business Continuity	**Yes**	**No**	**Comments**
Are the recovery procedures tested for efficacy?	☐	☐	
Are manual backup/restore procedures documented and practiced in	☐	☐	

case of automatic backup failure?			
Can you meet recovery time objective(s) (RTO) and recovery point objective(s) (RPO) for all products and services contracted with MassMutual?	☐	☐	
Is there a Business Continuity Plan?	☐	☐	
Monitoring	**Yes**	**No**	**Comments**
Do you monitor the security/policy violations and application/ networked services availability?	☐	☐	
Do you log successes and failures to access?	☐	☐	
Accounts Management & Access Control	**Yes**	**No**	**Comments**
How will MMFG data be secured at your site?			
Will MMFG data be accessible from Internet?	☐	☐	
Who will have access to MMFG data?			
How do you prevent other clients accessing MMFG data?			
How and where are user IDs and Passwords stored? How secured?			
Will the access credentials be encrypted when passing through public network?			
Do you employ any mechanisms that facilitate secure data exchange?			
E-Commerce (applicable if vendor conducts business on-line)	**Yes**	**No**	**Comments**
Are the following maintained in e-commerce system:			
• Confidentiality?	☐	☐	
• Authorization?	☐	☐	
• Non-Repudiation?	☐	☐	
• Transaction Integrity?	☐	☐	
• Access codes encryption in storage and transmission?	☐	☐	

Additional information and comments: