Incident Response Log

#	Control:	Date	Documentation	Follow-up Documentation
1	Log Date:			
2	Date Reported:			
3	Date of Incident:			
4	Reported by:	Enter the name of the person whom you are talking with for the initial report.		
5	Description of Potential Incident:		As you're taking the call, describe what you can about the incident here.	Use this as the place where you develop a formal description of the incident.
6	Location of Data:		Describe the location of data here.	
7	User:	Enter the name of the person who was closest to the incident, or the user whom you want to be the primary contact for any investigation.		
8	User Location:			
9	User Contact Info:			
10	Witnesses:	Enter all the names of any employees, customers, or other users involved in the incident when possible and/or appropriate.		
11	System Affected:	Try to document all "information assets" or "containers of information" that have been affected.		
12	Employee(s) Affected:	Any names that wouldn't go in #7 and #10 above.		
13	Service Providers Involved:	List any and all potential service providers. As you work the incident, you might want to keep contact info here.		
14	Was customer information involved?	Yes, No, or Maybe		Finalize your formal statement about this here.
15	What type of information?	According to guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account numbers.		
16	How much information?			
17	Who has received this information?	Document who has received the information, if known.		
18	Is there any reason to believe recipient of information is "malicious?"	If you do not know who received the information, the answer to this is yes.		
19	Has misuse of this information occurred?			
20	Is it possible that misuse of information COULD occur?	If you do not know who received the information, the answer to this is yes.		
21	Initial Incident Classification:			

22	Incident Contained?	Enter the date that the incident was "contained" here.		
23	Escalation: ISO	Document the date that the Information Security Officer was first informed.		
24	Escalation: IRT	Document the date that the Incident Response Team was first informed.		
25	Escalation: BOD	Document the date that the Board of Directors was first informed.		
26	Escalation: Examiners	Document the date that the Board of Directors was first informed.		
27	Escalation History:		List all meetings called (time and date, attendees), here:	
28	Postmortem Review:			Document the date that a formal post-mortem review was conducted. Possibly include the location of the documentation.
29	Incident Closed:	Document the date that the incident was closed.		
30	Board Report Inclusion:	Will this incident be included in the board report? If no, put "not applicable." If yes, document the date of the report it was included in.		