Handling Cyber Security Incidents			
Process Number:	**DG27-P01**	Version Number:	**2.0**
Effective Date:	**14/01/2020**	Review Date:	**15/01/2021**

Author: Reviewers:	**David Pick, Network Security, IT Services** **Paul Smallcombe, Records & Information Compliance Manager** **Henrik Brogger, Head of IT Delivery, IT Services** **Kathy Whelan, IT Service Desk Manager, IT Services** **David Boakes, Assistant Director IT Operations & CISO** **Skender Osmani, Head of Client Devices, IT Services** **Richard Hughes, Customer Campus Support Manager Mile End** **Adam Thurston, Customer Campus Manager, Whitechapel** **Devin Singh, IT Service Desk Analyst** **Madalyn Hardaker, SMD, Information Governance Lead**

Authorisation:	
Name / Position	**IT Lead Team**
Signature	**IT Lead Team**
Date	**19/12/2019**

Revision History			
Version	Description	Author	Date
1.01	Review – No Change	Shelim Miah	07/08/14
1.02	Review and Update	Shelim Miah	23/09/19
1.03	Finalised	Shelim Miah	15/10/19
1.04	Feedback & Comments	Madalyn Hardaker	04/11/19
1.05	Title Change from IT Security Incidents	Shelim Miah	19/12/19

Purpose and Objective:	
To define the process for reporting and handling Information Technology (IT) security incidents. An IT security incident is any event affecting the security of any item of hardware or software that places any information processed or owned by Queen Mary, University of London at risk of loss, unauthorised disclosure or unauthorised alteration, including destruction, or which risks unauthorised access to or control of any IT resource or associated infrastructure. In this context "IT resource" includes items of IT equipment, accounts allowing access to any IT system (QMUL or otherwise), and configuration parameters of any IT system.	
Trigger:	Cyber security incident detected
Inputs:	Register of Systems Containing Confidential or Restricted Data
Outputs:	IT Security Incident Log updated Remedial Actions Incident Report

References:
DG-WI-05-01 – Information Security Incident Reporting SOP DG05 – Information Security Incident Reporting SOP DG09 – Information Classification SOP DG27 – IT Security Incident Management Information Commissioner's Guidance on Data Security Breach Management

Queen Mary University of London

Process Steps

	Responsibility	Activity
1.	Person who discovers an incident	**Immediate Containment and Recovery** When an information security incident is detected, ascertain whether the incident is still occurring. If so, steps must be taken immediately to minimise the effect of the incident, for example by alerting relevant staff, shutting down a system, removing media, securing a physical area or equipment.
2.	Person who discovers an incident	**Incident Reporting** The person who discovers or receives a report of an incident must inform the IT Service Desk by: e-mail: servicedesk@qmul.ac.uk Telephone: 020 7882 8888 Raise a ticket: https://servicedesk.qmul.ac.uk Where the Incident is outside of central IT Services control, it should be reported to the local IT manager or their equivalent within the area the incident occurred.
3.	IT Service Desk	The IT Service Desk shall log a ticket in the IT Service Management Tool (ITSM) and allocate it to the IT Security Incident Team by assigning the ticket to the appropriate queue. The IT Service Desk shall ensure the Information Security Manager is made aware of the reported incident.
4.	Information Security Manager	The Information Security Manager shall assess the incident and assemble the IT Security Incident team to investigate. This may consist of the Records and Compliance manager, local Information Champions or equivalent and other IT staff delegated by the IT Services department.
5.	IT Security Incident Team	**Initial Assessment** An initial assessment of the incident is carried out to determine the scope of the incident. Taking into account: • The number of users (both inside and outside QMUL) that are affected (even if "only" by lack of service) • The number of computer systems affected • Degree of compromise • The nature and classification of any data sets • Cross reference the above data against the register of systems holding confidential or restricted data • Any data and its classification accessible by the affected computer system

		If the systems managers of these systems have not already been informed of the incident they must be informed at this point and any suitable remedial actions taken with reports made back to the IT Security Incident Team.
6.	IT Security Incident Team and or Service Desk	If it is determined at step (5) or step (3) that information may have been compromised or suspected of being compromised during the incident (for example, there is sensitive data at risk) then the QMUL Information Security Incident Team must be informed by: e-mail: information-security@qmul.ac.uk In this case DG05-P01 shall subsequently be followed in parallel.
7.	IT Security Incident Team	**Assign Incident Manager** An Incident Manager is appointed (normally the Information Security Manager) in conjunction with the QMUL Information Security Team if appropriate. Normally there will be one Incident Manager for any one incident even if both procedures are being followed because the incident has both general Information Security and IT Security aspects.
8.	Incident Manager (or other qualified person)	**Determine Incident Severity** Each incident will be evaluated to determine its severity in terms of both Information Security and the security of the Information Technology. The final grade for an incident will be determined by the evaluation that gives the more serious grade. The evaluation of potential adverse effects will include how many computer systems and people are affected, the seriousness of any consequences and the likelihood of these happening, and must consider: • How many records are affected? • What type of information is involved? • Is it protected e.g. with encryption? • What has happened, or might have happened, to the information? • How many computer systems have been affected? • How many people have been or are likely to be affected even if only by a lack of service? • What harm can come to any individuals? • Are there risks to safety, financial loss, loss of reputation, or to public health? • Are there any other wider consequences? Incidents shall be graded as indicated in Appendix B.

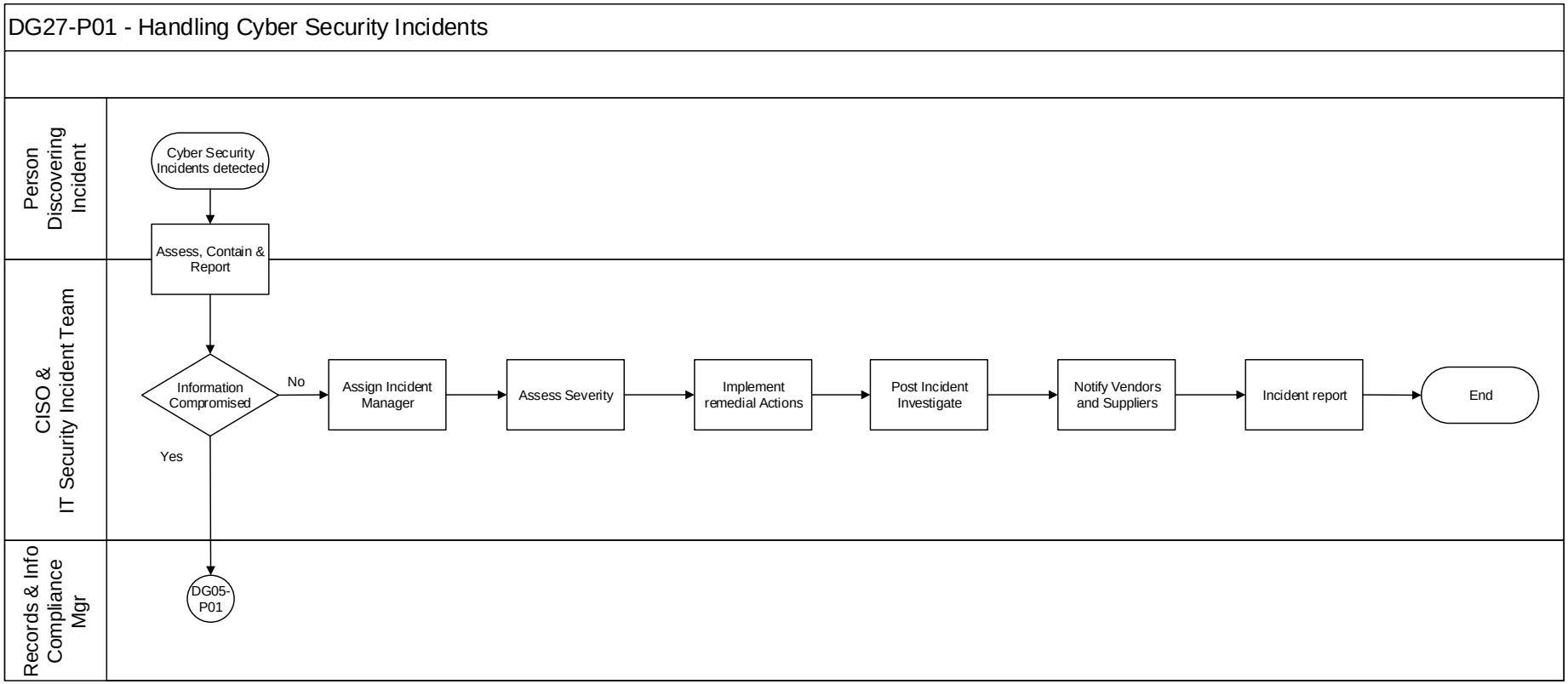
9.	QM IT Security Incident Team	**Incident Management** This step is taken as both part of this work instruction and as part of DG05-P01. For Grade 3 and 4 incidents, once immediate remedial action has been taken and the incident logged no further action will be required. Update the IT Security Incident ticket/Log and close the incident.
10.	Incident Manager / QMUL Security	This step is taken as both part of this work instruction and as part of DG05-P01. For Grade 1 incidents where illegal activity is known to have, or is believed to have, occurred, or for Grade 1 or 2 incidents where there is a risk that illegal activity might occur in the future, it may be appropriate to contact the police. QMUL Security, who can be contacted on 020 7882 5000, will initiate the contact with the police as necessary. In any case, Grade 1 incidents will be escalated to the Academic Secretary & Secretary to Council and other senior management as appropriate. Grade 1 and Grade 2 incidents will be escalated to the Chief Information Officer (CIO) and other IT Services management as appropriate.
11.	Incident Manager and IT Systems Managers	**Review Actions Taken** If sensitive data is involved there will be actions taken as part of DG05-P01 with respect to the data itself. The actions detailed here are about safeguarding the underlying information technology. The Incident Manager must review any steps already taken to recover any losses and limit damage, and initiate further steps as necessary at this point which might include, but are not limited to: a) Attempting to recover lost equipment b) Securing physical locations c) Contacting other relevant QMUL departments, so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information about any individuals whose data has been compromised. Consideration should be given to a global email. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the IT Security Team d) Contacting the Communications Office so that it can be prepared to handle any press enquiries e) Powering down or removing compromised

		equipment f) The use of back-ups to restore lost/damaged/stolen data g) If an incident includes the disclosure of any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed h) If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use i) Applying patches to systems or inhibiting functionality to eliminate or reduce the risk of similar incidents in the future
12.	Incident Manager	**Investigation** In most cases the next stage would be for an assigned Investigator to fully look into the incident. The Incident Manager shall assume or appoint this role. S/he should ascertain what and whose data was involved, the potential and actual effect on any data subjects and what further steps need to be taken to remedy the situation.
13.	Incident Manager	The investigation should consider: • The type of data, • Its sensitivity, • What protections are in place (e.g. encryption), • What has happened to the data, • Whether the data could be put to an illegal or inappropriate use, • How many people are affected, • What type of people have been affected (the public, suppliers etc.) • Whether there are wider consequences such as whether it can be re-used (e.g. for fraudulent purposes). A clear record should be made of the nature of the incident and the actions taken in as much detail as possible in the IT Security Incident Log.
14.	Incident Manager	The investigation should be completed urgently and wherever possible within 24 hours of the incident being discovered or reported. A further review of the causes and recommendations for future improvements can be done once the matter has been resolved.
15.	QMUL Information Security Incident Team and IT Systems Managers	**Notification** The notification of people and authorities about information loss is dealt with as part of DG05-P01 but there are other notifications that may need to be made with respect to the Information Technology. These include: • The supplier of any software that may have been

		found to contain a fault • The User Groups for any software that may have been found to contain a fault Some people and/or agencies may need to be notified as part of the initial containment and management. However, the decision about who to notify will normally be made once an investigation has taken place. Update the IT Security Incident Log.
16.	QM IT Services Information Security Manager	**Review and Evaluation** For Grade 1 and 2 incidents, once the initial aftermath of the incident is over, the QMUL IT Services Information Security Manager shall fully review both the causes of the incident and the effectiveness of the response to it.
17.	Incident Manager	**Write Incident Report** An incident report should be written and sent to the IT Services Information Security Manager to include: • Description of events indicating specific timelines • Personnel involved • How it was discovered • Activities leading up to the incident • Impact on QM and other parties • Decisions and actions taken • Problems encountered • Successful and unsuccessful activities • Notifications required • How notification was undertaken, • Steps taken for containment and remediation • recommendations for prevention • Identification of policy or procedure gaps • Results of post-incident review.
18.	QM IT Services Information Security Manager	**Check Remedy Taken** The IT Services Information Security Manager shall check that any remedy has been taken. This is not necessary for Grade 3 or Grade 4 incidents. In the case of Grade 1 and 2 incidents the incident report will be communicated to senior management if they have not already been informed as part of any previous stage. The incident will then be closed.
19.	QM IT Security Incident Team	If systematic or on-going problems are identified then an action plan must be drawn up to remedy these, especially any identified need for training. If the incident warrants a disciplinary investigation, the manager leading this should liaise with Human Resources for advice and guidance. If the law has been broken then legal proceedings may also result. Certain incidents, such as those involving fraud, may also have to be notified to QMUL's internal auditors. In any of

		these cases it will be necessary to collect and preserve evidence to an appropriate standard.

Appendix A


DG27-P01 - Handling Cyber Security Incidents
Person Discovering Incident
CISO & IT Security Incident Team
Records & Info Compliance Mgr
Cyber Security Incidents detected
Assess, Contain & Report
Information Compromised
No
Yes
Assign Incident Manager
Assess Severity
Implement remedial Actions
Post Incident Investigate
Notify Vendors and Suppliers
Incident report
End
DG05-P01

Appendix B – data to be captured in the IT Security Incident Log

1. Incident Number
2. Date of Incident (if known)
3. Discovered by
4. Email address
5. Date / Time of Discovery
6. Reported to IT Incident Team by
7. Date / Time Reported
8. Identifications of IT systems and resources at risk
9. Description of Information at risk (include data set references if available)
10. Classification of the most sensitive Information
11. Owner(s) of data sets
12. Which Department(s)
13. If and when reported to the (general) Information Security Team
14. Identities of any third party is involved
15. Description of Incident (how discovered, impact etc.)
16. Immediate Remedial Action Taken
17. Severity Grading
18. Investigator
19. Date appointed
20. Result of investigation
21. Action plan

Appendix C –Incident Grades

Grade	Description
Grade 1	This is for illegal activities which must be notified to a law enforcement agency.
Grade 2	This is for serious incidents which impact on a significant number of IT systems or users or Data Subjects (as defined by the Data Protection Act).
Grade 3	This is for low level/routine incidents where the impact is limited.
Grade 4	This is for low level/routine incidents where the impact is negligible and there is no general Information Security impact. This grade is not appropriate if the incident is also being dealt with as an Information Security Incident and DG-WI-05-01 has been activated.

Queen Mary University of London

Appendix D – Example Incidents and Assigned Grades

The following table lists example incidents and the grades that are likely to be assigned to each to assist with the grading process in step 6.

Ref	Description	Grade	Why?
1.	A notice is received stating that a machine in the College has been involved in the distribution of copyrighted material	3, 4, or none	If the copyrighted material was being distributed by software installed knowingly by the manager/owner of the machine then it is not an IT Security matter but a disciplinary one. If the software performing the distribution was installed without the manager's knowledge then it is malware and the vector used to install it needs to be located and blocked.
2.	A notification of a virus infection on a student's personal laptop in the Halls.	4	No likely impact on QM systems, data, or operations.
3.	A notification of near-simultaneous virus infections on students' personal laptops in the Halls.	3	Little likely impact on QM systems, data, or operations; but there is likely cross-contamination between the student PCs and the possibility that this might spread to other QM systems.
4.	A report of a virus infection on a centrally-managed staff computer.	3 or 2	If the computer is centrally managed it should have up-to-date anti-virus software that should have stopped the infection. Other, similar, computers are probably at risk and need to be protected against the infection vector.

Ref	Description	Grade	Why?
5.	Multiple near-simultaneous reports of virus infections on centrally-managed staff computers.	2	This is likely to be a new, 0-day, vulnerability and the infection vector needs to be identified and blocked. There will also be a considerable effort required to clean up each infected machine. Some College operations may well be inhibited until this is complete.
6.	Pornographic images or other offensive (terrorist, racist, or hate promoting) material found on a desktop computer.	1 or none	For some extreme pornographic images simple possession is a crime and Grade 1 is applicable. For the others, provided their presence can be explained by human action this is not an IT Security issue (although it may well be a disciplinary issue).
7.	Pornographic images or other offensive (terrorist, racist, or hate promoting) material found being made available by a server run by the College.	1, 2, 3, or none	For some extreme pornographic images simple possession is a crime and Grade 1 is applicable. If the server has been “hacked” and the offensive material inserted into normally published material Grades 2 or 3 may be applicable depending on how widely the material has been exposed. If the server has not been “hacked” then this is not an IT Security issue (although it may well be a disciplinary issue).
8.	SPAM E-Mail messages being sent directly from a student's personal machine by malware.	4 or 3	The likely impact on QM operations is minimal unless the volume has been high, in which case the grade should be raised from 4 to 3.
9.	SPAM E-Mail messages being sent from a student's personal machine by malware that are routed via a College server.	3 or 2	There is a likely impact on QM operations because the College server that is forwarding the messages is in danger of being blacklisted and this is likely to affect E-Mail from other users routed through the same server.

Ref	Description	Grade	Why?
10.	SPAM E-Mail messages being sent directly from a managed staff machine by malware.	3	The malware should never have been able to run, and the cause should be identified and blocked. Operation impact is still likely to be fairly limited.
11.	SPAM E-Mail messages being sent from a managed staff machine by malware that are routed via a College server.	3 or 2	The malware should never have been able to run, and the cause should be identified and blocked. There is also a likely impact on QM operations because the College server that is forwarding the messages is in danger of being blacklisted and this is likely to affect E-Mail from other users routed through the same server.
12.	SPAM E-Mail messages are being sent through our Webmail service using a specific account. The user admits to falling for a “spear-phishing” fraud.	3 or 2	Accounts can be used for accessing multiple services and any of the services that can be accessed using the account used could have been accessed. Logs should be checked to determine if any sensitive services were accessed by the attackers. Passwords must be changed. The grade assigned to such an incident will depend on the classification of the most sensitive data that might have been accessed using that account name and password.

Ref	Description	Grade	Why?
13.	SPAM E-Mail messages are being sent through our Webmail service using a specific account. The user does not admit to falling for a “spear-phishing” fraud or telling anyone else their password.	2	Accounts can be used for accessing multiple services and any of the services that can be accessed using the account used could have been accessed. Logs should be checked to determine if any sensitive services were accessed by the attackers. Passwords must be changed. The assumption must be made that the credentials were obtained by some sort of malware and every computer the user has used quoting this username and password must be checked before the new credentials can be used. The amount of work involved in sorting out this type of problem means it must be reported as a Grade 2 incident.
14.	Computing platform availability problem, for example power failure, air-conditioning failure, disc failure, electronic failure.	2, 3, or 4	This can't be a Grade 1 incident, but depending on the number of users affected and the impact on College business it might be any grade from 2 to 4.
15.	Computing platform availability problem caused by a denial-of-service attack.	1 or 2	Grade 1 might be appropriate because a denial-of-service attack is illegal but it is not a crime that **must** be reported, and so Grade 1 may not be appropriate.
16.	Computing platform availability problem caused by an unknown underlying problem.	1, 2 or 3	Grade 4 is inappropriate here because the impact is unknown and the cause might spread. Grade 1 would be appropriate if the problem is the result of an attack of any sort.

Ref	Description	Grade	Why?
17.	Corruption of data caused by a machine failure.	2, 3, or 4	Grade depends on the number of users affected and the impact on College business before service is restored, and the degree of roll-back necessary to restore from backups.
18.	Corruption of data caused by a software failure.	2, 3, or 4	Grade depends on the number of users affected and the impact on College business before service is restored, and the degree of roll-back necessary to restore from backups. The likelihood of a repeat incident is also a factor.
19.	Corruption of data caused by an unknown underlying problem.	1, 2, 3, or 4	Might be grade 1 if the underlying problem turns out to be an attack of some sort, otherwise the same sort of criteria apply as immediately above. It is not necessarily a crime that **must** be reported, and so Grade 1 may not be appropriate.
20.	Unauthorized change to data made by a person.	1, 2, 3, or 4	This is only an IT Security incident if the person should not have been able to access the system to make the change. Otherwise this is an Information Security Incident. If the change was deliberate it could be a grade 1 incident; and in any case almost certainly a disciplinary matter. It is not necessarily a crime that **must** be reported, and so Grade 1 may not be appropriate.
21.	Unauthorized change to data from an unknown cause.	1, 2, or 3	Grade 4 is not appropriate because there is not certainty about the consequences of the change, or about the likelihood that other changes might have the same cause.

Ref	Description	Grade	Why?
22.	Theft of a device or any media containing only encrypted data	1 or 3	There is a crime that should be reported. It is not necessarily a crime that **must** be reported, and so Grade 1 may not be appropriate.
23.	Theft of a device or any media containing any unencrypted data	1 or 3	If the stolen device or media did not contain any sensitive data then there is not an IT Security Incident. If any of the data was sensitive then there is an issue about how the sensitive data was stored there in an unsafe manner. This might be an IT technology failure, or might be the result of a person not following proper procedures (which can be a disciplinary matter). There is a crime that should be reported. It is not necessarily a crime that **must** be reported, and so Grade 1 may not be appropriate.
24.	Loss of a device or any media containing only encrypted data	3 or 4	Whilst information is unlikely to have been put at risk, the incident should be recorded so that any appropriate lessons can be learned from it.
25.	Loss of a device or any media containing any unencrypted data	1, 2, or 3	If the lost device or media did not contain any sensitive data then there is not IT Security Incident. If any of the data was sensitive then there is an issue about how the sensitive data was stored there in an unsafe manner. This might be an IT technology failure, or might be the result of a person not following proper procedures (which can be a disciplinary or even criminal matter).

Ref	Description	Grade	Why?
26.	Use of another person's credentials to gain access to systems or services.	1, 2, 3, or 4	Grade would be 1,2,3,4 on the basis it could be simple ignorance that needs to be remedied by pointing the user at our regulations. At the other end of the scale, it could be a serious hack. In between, compromised accounts are used for spam/phishing when the users give out the information themselves in response to a phishing email.

Appendix C – IT Incident Report Template

1. Incident Detail			
Incident Title		Incident Reference	
Author of report			
Role			
Contact details			
Date & time of Incident			
Incident Grade	1 ☐ 2 ☐ 3 ☐ 4 ☐		

2. Incident Description. (when, what happened and who was involved)

Provide a brief description:

3. How was the Incident detected? (include activities leading up to the incident)

4. Impact / Potential Impact Check all of the following that apply to this incident.

- ☐ Loss / Compromise of Data
- ☐ Damage to Systems
- ☐ System Downtime
- ☐ Financial Loss
- ☐ Other Organisations' Systems Affected
- ☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
- ☐ Violation of legislation / regulation
- ☐ Unknown at this time

Provide a brief description:

5. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

☐ Public ☐ Internal Use Only	☐ Restricted / Confidential (Privacy violation) ☐ Unknown / Other – please describe:
Provide a brief description of data that was compromised:	
6. Who Else Has Been Notified?	
Provide Person and Title:	
7. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.	
☐ No action taken ☐ System Disconnected from network ☐ Updated virus definitions & scanned system	☐ Restored backup from tape ☐ Log files examined (saved & secured) ☐ Other – please describe:
Provide a brief description of response taken:	
8. Further Details	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Problems issues encountered	
Failings that lead to the breach	
Recommendations for prevention	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	