Cyber Digital Forensic Readiness (DFR) Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	09/01/2017
V 0.2	Mick Jenkins	Formatting Amendments	10/01/2017
V 0.3	Andrew Clarke	Amendments from PWG/CSIRT – disable Wi-Fi, add MAC devices, clone copy disks	23/02/2017
V 1.0	Andrew Clarke	CISA Approval	07/09/2018
V 1.1	Andrew Clarke	Add 5.12.1 Integrity of the data / Evidence file; Write-Blocker	10/02/2020
V 1.2	Andrew Clarke	Appendix B – DFR Ransomware	22/04/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This policy sets out the context and process for Cyber Forensic Readiness in Brunel University London.

The purpose of this policy is to ensure that:

- Brunel University London requirements relating to security and confidentiality of equipment and information and the requirements of the Data Protection Act are met, protect the University, its staff and its students through the availability of reliable digital evidence gathered from its systems and processes;

- Allow consistent, rapid investigation of major events or incidents with minimum disruption to University business;

- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required;

- Demonstrate due diligence and good governance of the University's' information assets.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Head of Security	Is responsible for providing all forensic evidence required in an acceptable format
Chief Information Security Officer	Is responsible for ensuring all parties comply with policy during investigation.
Cyber & Information Security manager	Owner of the policy.

3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A16 – Information security incident management.
ISO 27001:2013 Conformance Control	Information Classification Objective A.16.1.7 Collection of Evidence.

1.4 Scope

This policy applies to:

- All University data held on any medium, including all forms of hard copy and electronic data;
- All University Colleges, Research Institutes, Administrative and Service Departments;
- All contractors, third party suppliers and external stakeholders.

Brunel University London provides the infrastructure at Data Centres in support of the Brunel University London services. Other providers to Brunel University London maintain their own computer system and network, although there may be interconnectivity between the different providers. This policy applies only to the systems and networks used by Brunel University London at the Brunel University London occupied Data Centres.

This Policy applies to all locations from which University information is accessed including off-campus use. As the University operates internationally through its locations abroad, the remit of the Policy shall include such locations and shall pay due regard to non UK legislation that might be applicable.

1.5 References

BUL-POL-IRM01 Information Risk Management Policy

BUL-POL-16-1 Infosec Incident Management

BUL-PROC-16-02 Infosec Incident Management Procedure

BUL-POL-6.1.1 - InfoSec Roles

1.6 Benefits

The benefits to the University of creating a forensic readiness policy comprise the following:

- Enterprise defence mechanisms are captured;
- Acts as a deterrent to insider threats In the event of an incident, this would enable minimum disruption and also link in to the University's Business Continuity plans;
- Reduced cost and time for internal investigations;
- Extends information security to the wider threat from cyber-crime;

- Demonstrates due diligence and good enterprise governance arrangements;
- Compliance with the Brunel University London ISO27001:2013 and other regulatory requirements;
- Improve the prospects for successful legal action if required;
- Supports employee sanctions based on digital evidence.

2.0 Introduction

2.1 Forensic Readiness

Forensic readiness is a key component of Brunel University London information risk. This will maximise the University's potential to use digital evidence whilst minimising the cost of an investigation.

This policy reflects the high level of importance placed upon minimising the impacts of information security incidents and safeguarding the interests of students, staff and the University.

2.2 Forensic Accountability / Responsibilities

Heads of Colleges / Institutes / Service / Managers (Data Stewards – DS) ref. BUL-POL-6.1.1 - InfoSec Roles

Heads of Colleges/Institutes/Service/Managers are responsible for ensuring that their service operates within the Information security management system framework. They will ensure that:

- There are effective methods for communicating Information Governance related issues within their service.
- Staff attend relevant training, induction and mandatory updates in relation to Information Governance along with ensuring that staff complete the necessary training required annually.
- Staff are aware of and adhere to Information Governance policies. Necessary risk assessments are undertaken within their area of responsibility.
- Information Governance issues and risks are discussed in directorate / team meetings.
- Incident reporting is integral to the operational activities within their areas and all incidents are reported and investigated in accordance with Brunel University London policy. BUL-POL-16-1 Infosec Incident Management

Security Operations Manager
The Security Operations Manager is responsible for coordinating the development and maintenance of forensic policy procedures and standards for the University.

The Security Operations Manager is responsible for the on-going development and day-to-day management of the forensic policy within Brunel University London's overall Risk Management Programme.

Data Custodians (DC) ref. BUL-POL-6.1.1 - InfoSec Roles

Data Custodians are defined as the Information Asset Owners (IAO) who shall ensure that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned ownership. Goals for forensic planning include:

- Ability to gather digital evidence without interfering with business processes;
- Prioritising digital evidence gathering to those processes that may significantly impact the University, its staff and its students;
- Allow investigation to proceed at a cost in proportion to the incident or event;
- Minimise business disruptions to the University;
- Ensure digital evidence makes a contribution on the outcome of any investigation, dispute or legal action.

DCs shall submit their plans for forensic readiness, to the Security Operations Manager for review along with details of any planning assumptions or external dependencies.
Forensic readiness plans shall include specific actions with expected completion dates.

Cyber & Information Security Manager

Will be responsible for:

- Issuing guidance for implementing and compliance with the Forensic Readiness Policy;
- Monitoring performance through quality control and internal audits;
- Identifying where improvements could be made;
- Reporting performance standards to the Information Governance Group.
- Defining the business scenarios that may require digital evidence including:

1. Employee Internet misuse / abuse
2. Employee Email Misuse / abuse
3. Electronic bullying / harassment
4. Formal Police / legal request for digital evidence
5. Fraud
6. CCTV
7. Production of audit logs
8. Back up data
9. Removable media
10. Network intrusion / prevention audit records such as cyber-attacks (hacking attempts etc.)
11. Mobile phone and desk phone investigation

All staff

Be aware of and adhere to relevant information governance policies and procedures

Complete mandatory Information Security training.

Intended Users

It is the responsibility of all staff (including those on temporary or honorary contracts), agency staff and students to comply with this policy.

Compliance with Brunel University London policies is a condition of employment, and breaching a policy may result in disciplinary action or lead to prosecution under UK law.

3.0 Policy Compliance

The Forensic policy complies with the requirements of the following University polices

- Internet
- Email
- Information Lifecycle and Records Management
- Data Protection Policy
- Incident Reporting
- Data retention
- Acceptable Use

4.0 Incident Reporting

Incident Reporting (including near miss)

Incidents (or near misses) that constitute any actual or potential breach of data confidentiality must be reported directly to the Information Access Officer and the appropriate University Information Governance teams immediately.
An Incident Form must be completed and submitted in accordance with Brunel University London procedures.

5.0 Forensic Plan Execution

5.1 Component Specifics

The components that have been identified as potential sources of digital evidence (please note that this list is not exhaustive and shall be reviewed and amended by the University Cyber & Information Security Manager) can be classified as:

- Wintel machines, hard disk and system logs
- UNIX machines, hard disk and system logs
- Firewalls producing logs readable by a PC
- IDS producing logs readable by a PC
- Network equipment producing logs readable by a PC
- Door/gate entry systems
- Monitoring equipment such as CCTV
- Apple MAC devices
- External removable storage media
- Mobile devices (iOS, Android, Blackberry)

5.2 Tools

The Cyber & Information Security Manager shall, in conjunction with the Head of Security, identify and seek procurement of tools (e.g. EnCase Forensic™) and or equipment to achieve the following:

- Data capture
- Image capture (e.g. operating system and configuration)
- Secure storage on media.
- Secure physical storage of media.

The use of the above tools shall be documented by the Cyber & Information Security Manager.

5.3 General Guidance

It is not possible to cover all possible scenarios for security incidents. The following is provided as guidance in preparing for a forensic investigation.

5.4 Independent Witnesses

All actions that are taken in this plan are under the Two Persons Present rule (TPP) unless otherwise stated. One of these persons shall be the Head of Security or Security Operations Manager (or their recognised deputy) and the second shall be a trusted person not involved with the system under

investigation from the Technical teams. These persons shall monitor each other and jointly sign evidence as required below.

5.5 Contemporaneous Notes

DOCUMENT EVERYTHING THAT IS DONE.
A Property/Exhibit numbering scheme shall be defined for all potential evidence.

Concise, accurate and contemporaneous hand written notes shall be taken, in ink, of everything done from the time that a suspected incident is reported or discovered until all evidence is collected and forensically sealed.

These notes may be used for:

- Witness Statements;
- Police or other law enforcement agency briefing;
- Briefing Notes;
- Incident Response Reports;
- Internal Investigations;
- Criminal or Civil Evidence.

These notes shall be in the form of a chronological event log that includes:

- Date;
- Time;
- Persons involved;
- Persons informed;
- Activity or observation;
- Place of creation of related documents;
- Timestamps, digital signatures shall be obtained for digital evidence and recorded as having been taken in the log.

Interview notes shall be typed up and reviewed by the interviewee as soon as practicable and signed by the witness and interviewers.

5.6 Forensically Secure the Scene

Specialist forensic guidance, in conjunction with the Security Operations Manager, shall be sought here.

5.7 Isolate the relevant machines/area

Disconnect all network, Wi-Fi and modem cables to prevent remote access to the machine (either across a network, wireless or via a modem) destroying or altering potential evidence. Include in the event log any connected drives or other storage media before disconnection.

If the system is a Virtual system (VM), physical disconnection is not possible, in this situation, cloning can be applied to isolate the system in question.

Exclude unauthorised personnel from the vicinity of a suspect machine to prevent intentional or unintentional compromise of potential evidence on a suspected machine by changing or destroying or even encrypting records.

Only a minimal number of authorised staff members are to be given access to the area in which the machine is kept. Any individual who insists on being given access to a suspect machine (e.g. senior managers) shall be informed that notes in relation to their access will be recorded and that they will be invited them to sign these notes upon completion of their activities.

In making these notes, investigators are to ensure that the notes are concise, accurate and contemporaneous, and that they contain:

- The name of the individual requesting access;
- The date and time of the request;
- The reasons given for insisting on access;
- Actions performed including systems accessed, activities undertaken in that system, and any input used;
- The date and time this person left the area;
- The name of the escort.

If the individual declines to sign these observations, the investigator is required make a note to that effect and if possible ask for a reason for non-signing and include the response in the recorded information.

5.8 Determine what the machines are/were doing

If the computer is powered down, leave it in that state. If the machine is powered up, make a record any activity that is evident.

In particular record:

- What operating system(s) is (are) running;
- What applications are running;
- Any documents/files that may be open in a word processor or other application;
- What system processes are running;
- Check any URLs being accessed if an Internet browser is open or Newsgroups being accessed. If possible, photograph or video the screen displays encountered.

If any documents are open in word processing software or other applications, save these to read only media in versions that save and do not save changes. This is to prevent loss in a subsequent system shutdown. If possible, save

'before' and 'after' versions that can be studied for changes. Correctly label storage media and store securely.

5.9 Shutdown

If the computer is running and will not need transporting for forensic examination, it may be decided not to shut it down. If it needs to be shutdown, before doing so ascertain the following:

- Will shutting it down prevent access to password protected data that may be accessible at that time (for example encrypted files or hard disk drives);
- Is the user name and password of a network computer known;
- Is shutting it down going to cause considerable disruption to the University business;
- Is the computer in the process of carrying out a critical legitimate function;
- Is shutting it down going to alert other potential staff members or suspects to the discovery of the incident;
- Have the shutdown/boot up scripts been modified to corrupt evidence.

Before shut down, capture and record system information that may be lost in the shut down or not captured during the execution of the backup procedure. This includes:

- All current network connections;
- All current system processes;
- Active users currently logged on;
- All open files (files may be deleted if a process exits when the network is disconnected);
- Any other volatile data that may be lost

If it is determined that shutting down the computer is safe and necessary, then shut down the computer, ensuring that the process is as 'graceful' as possible.

5.10 Search the Scene

Search the area carefully for external disk storage, CD-ROMs, zip disks and other removable media that could have been be stored or hidden. When conducting a search for these items – make notes of the area searched, what was found, and by whom. Where possible, photograph or video record the items in situ, before they are removed and labelled. Trace and examine all network cables, and look for written down passwords, particularly under desks or chairs. Account for any items that should not normally be present.

If the suspected staff member is present, make careful witnessed (TPP) notes of anything said. Ask the staff member for passwords and other relevant details during the initial interview with them. Once again, make careful notes of any

conversations and make sure that there is another person present to corroborate what was said. This could be critical to the subsequent investigation

5.11 Record the Scene

Photograph and/or video record the suspect machines in situ including all cabling. Photos and videos must show the date and time even if it has to be written on something and displayed within the frame.

Make a sketch of the area / room in which the suspect machine is located, noting where the machine and other furniture is sited, where personnel were standing upon arrival of the investigators, and any other identifying items that may assist specialists in any subsequent investigations.

Label all hardware, cables and also the sockets from which they were removed before disconnecting, in a manner that makes it easy to identify the original location of the items and using the defined numbering scheme. This will assist in the reconstruction of the system to its original configuration later, and may assist others with understanding its configuration.

Collect and label all removable storage media, secure all USB devices, CD-ROMs etc., and note the location in which they were found, using the defined numbering scheme.

Label all computers, hardware and cables using the defined numbering scheme.

5.12 Seize the Evidence

Ensure that all components and peripherals related to the computer being seized are also taken. There may be only one opportunity to gather all the available evidence for further investigation or action. Leaving behind computer equipment or software may make further investigation difficult, or allow evidence to be destroyed. When removing equipment and / or components consider:

- If seizing laptop computers, PDAs or other memory retention devices, ensure the associated power supply is seized. Ask for passwords.
- Collect all necessary computer storage media such as USB drives, hard disk drives, floppy disks, CD-ROMs, backup tapes and any unusual or suspected software such as encryption programs.
- Collect all relevant manuals or other documentation related to the computer hardware, software or peripheral equipment. These may be required by forensic specialists later.
- Keep magnetic media, such as external storage, separate from other items seized and away from magnetic and radio sources.
- When seizing items, only group items together if they are found together.
- Do not mix many similar items (for example disks) found in different

locations, with the intention of sorting them out later. Many computer related items such as disks look the same and later on it may be impossible to differentiate between items found at different locations.

After all the necessary items have been seized, they must be preserved, which means:

- Pack the items with care;
- Transport all equipment with care;
- Do not turn on equipment or attempt to operate it Do not open computer bodies or attempt to remove hardware Protect volatile evidence.

5.12.1 Integrity of the data / Evidence file

Digital evidence can be cited as evidence in nearly every crime category. Forensic investigators need to be absolutely certain that the data they obtain as evidence has not been altered in any way during the capture, analysis, and control. Lawyers, judges and jurors need to feel confident that the information presented in a computer crime case is legitimate.

In computer forensics, an evidence file is data that has been put into a special image format with a forensic software tool, such as EnCase® Forensic, X-Ways Forensics® and Sleuthkit Autopsy®. The purpose of creating an evidence file is to have a copy of a suspect's media so the investigator does not contaminate the original media. If the original media were investigated instead of the evidence file, a lawyer could argue that the investigator altered the media to incriminate their client. Creating the evidence file helps to ensure that the examined media has not been tainted by an investigator. The primary purpose of an investigator creating a separate evidence file is to ensure the original media does not become altered or contaminated when the technician conducts the forensic investigation.

To facilitate this non-repudiation, a write-blocker should be used to gather digital intelligence.
A write-blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data and are commonly used when acquiring a suspect's media. When a drive is connected to an operating system, changes are made to that drive; write-blockers will prevent Windows or other operating systems from writing to that drive.
If a drive is connected to a system without a write-blocker and changes were written to the drive, the drive is contaminated. Any contamination could leave some doubt in a jury's mind.
Connecting the write block solution
There are two basic types of write blockers:

- Hardware write blocker—The hardware blocker is a device that is installed that runs software internally to itself and will block the write capability of the computer to the device attached to the write blocker.
- Software write blocker—The software blocker is an application that is run on the operating system that implements a software control to turn off the write capability of the operating system. If you are using a software write

blocker, ensure to attach the external evidence collection drive prior to activating the software blocker as this will allow the external drive to be written to.

If you are collecting data from a USB device such as a thumbdrive, you need to activate the software or hardware blocker prior to connecting the device to the collection system. Importantly, make sure that you have already connected the external evidence collection drive and prepared it.

5.13 Preserve the Chain of Custody of Evidence

Specialist legal advice must be obtained but a list of considerations is described below.

A complete account must be kept of what has happened to each piece of evidence that may be tendered in court proceedings. Carefully maintaining this chain of custody is required not only to protect the integrity of evidence, but also to make it difficult for a lawyer/solicitor to successfully argue that the evidence was tampered with while it was in Brunel University London custody.

The chain of custody procedure is a process of documenting the complete journey of evidence during the lifetime of the case. When the evidence is collected, create a register that details all items to be used as potential evidence. This register shall then be used to record any movement or action taken on any item. The details for each piece of evidence recorded in the register shall show:

- Who collected it;
- How and where it was collected;
- Who took possession of it;
- How was it stored and protected;
- Who accessed it, for what purpose, and the date and time of such access;
- Who removed it, for what purpose, and the date and time of removal and return;
- Details of any forensic procedures that were carried out (out of scope for this document but included for completeness).

The fewer people who have access to evidence the better.

Any evidence collected must be stored in a secured area or container that accessible by as few people as possible, and only on a need-to-know basis.

The Cyber & Information Security Manager shall identify an evidence custodian who is responsible for the security of and access to the secure areas/storage containers so that evidence is available to demonstrate who has had access to it.

Whenever copies of electronic data are made, the original data, not the copy, shall then be sealed for evidence.
The original source disk(s) should be cloned using a method that guarantees the original is not altered, i.e. keeping the original write protected (using for instance a write-blocker).

Collectors of evidence shall

- Number, date, and sign notes and printouts.
- Seal disks with original, unaltered, complete logs in an envelope or other container; and then number, date, and sign the container.
- Copy original handwritten notes, and then seal the original notes as part of the chain of custody.
- Capture electronic data as soon as possible, and ensure that the process of making copies of the evidence has been witnessed.
- Ensure that closures have been secured with tamper evident seals.

The following rules shall apply:

- Access to labelled evidence shall be restricted to members of the incident response team and such access shall be for activities directly related to aspects of the ongoing investigation or subsequent prosecution.
- Any person granted access to labelled evidence shall record details of the access in writing in the register established for the purpose
- The recipient must issue a receipt for any labelled evidence.

5.14 Forensic Plan Closure

The activities in this plan shall be considered to be complete when the evidence collected for forensic examination has been delivered to the forensic investigation process.

Summary

Summary of Policy development process

The policy has been developed from Brunel University London requirements, previous Brunel University London policies on this topic, and with the collaboration of members of the Security Team.

Review and Revision Arrangements

The policy will be reviewed and revised on a regular basis (annually or as required by changing security or technical standards) by the Cyber & Information Security Manager.

Recommendations

While computer forensics is a specialised skill, it is important for us all to have a high level understanding of what is involved and the steps that should be taken during the course of an investigation.
In the event you have any reservation, and you are not comfortable to proceed with a possible forensic investigation, then please contact an in-house forensic expert.

Appendix A - Best Shutdown Procedures Based on Operating System in use

Operating System	**Characteristics**	**Shutdown Procedure**
Windows Server	Start button with Windows Symbol	Photograph the screen and note any running programs or messages, etc. **Use normal shutdown procedure.**
Windows 7,8, 10	Start button with Windows Symbol	Photograph the screen and note any running programs or messages, etc. **Pull the plug from the rear of the computer.**
Linux / Unix	If GUI present, look to Start button with Unix / Linux version symbol or icon, such as a red hat or fedora. If in console (no GUI), look to prompt for something like: [root@localhost root]# [user@host dir]$ If Mac use Apple symbol top left hand corner.	Photograph the screen and note any running programs or messages, etc. Use normal shutdown procedure. In many cases the user will need to be root to shutdown. Once at the terminal type synch;synch;halt If this is a MAC platform then pull the plug from the rear, unless it is running services such as web, Db then **use the standard shutdown process**

Appendix A – Digital Forensic Readiness Framework for Ransomware Investigation

Over the years there has been a significant increase in the exploitation of the security vulnerabilities of Windows operating systems, the most severe threat being malicious software (malware). Ransomware, a variant of malware which encrypts files and retains the decryption key for ransom, has recently proven to become a global digital epidemic. The current method of mitigation and propagation of malware and its variants, such as anti-viruses, have proven ineffective against most Ransomware attacks. Theoretically, Ransomware retains footprints of the attack process in the Windows Registry and the volatile memory of the infected machine. Digital Forensic Readiness (DFR) processes provide mechanisms for the pro-active collection of digital footprints.
This Procedure integrates the DFR mechanisms as a process to mitigate Ransomware attacks and is compliant with the ISO/IEC 27043 standard. The procedure mechanism has the potential to harness system information prior to, and during a Ransomware attack. This information can then be used to potentially decrypt the encrypted machine.