UNIVERSITY OF PORTSMOUTH

LOGGING NETWORK ACTIVITY

May 2016

Contents

Summary 5
What is this document about? 5
Who is this for? 5
How does the University check this is followed? 5
Who can you contact if you have any queries about this document? 5
1.0 Why keep activity logs? 6
2.0 Which logs should be collected? 6
3.0 How much activity should be logged? 7
4.0 Timestamps 7
5.0 Where will the logs be kept? 7
6.0 Who can read the logs? 8
7.0 How long should logs be kept? 8

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

This IS advisory describes the types of activity logs created to trace the use of Janet resources, to help investigate and learn from security incidents.

The University of Portsmouth must keep enough information to trace usage of Janet resources to specific computers or individuals on the University network at the request of Janet (normally Janet CSIRT) or Law Enforcement Agencies (this is consistent with the Janet Acceptable Use Policy (AUP) and Janet Security Policy).

Who is this for?

This IS advisory is aimed at all staff students, visitors and third parties using University network resources.

How does the University check this is followed?

Annual review of this IS advisory will be performed to evaluate its effectiveness.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

1.0 Why keep activity logs?

Logs should help you answer questions about activity on your network, for example:

- Who sent a particular e-mail?
- Can you confirm that a user of your network read this Web page on 23rd April?
- Are you able to confirm that a particular IP address downloaded this file?
- Please confirm can you isolate the source of this port scanning and make it safe.
- When was the last time that this computer was connected to the network?
- Who installed this unauthorised software on this computer?

1.1 What logs do Janet collect?

Janet CSIRT will know the remote IP address and destination port with which an IP address was communicating, or a URL or e-mail address identifying the remote entity. Janet CSIRT may also have other details - such as the TCP or UDP ports used or the volume of traffic. From this information the University of Portsmouth should, through its logs, normally be able to identify the computer involved and, if appropriate, the individual user.

2.0 Which logs should be collected?

2.1 Log data is collected for the following purposes:

a) Performance monitoring - Fault detection and alerting
b) Operational management - network troubleshooting, resource optimisation
c) Security - Intrusion detection and prevention
d) Incident analysis - root cause analysis using event log data
e) Audit purposes - privileged account access
f) Google logs - collected by Google in support of its privacy policy

a. Routers and firewalls

A router can export network flow records, which normally need processing to extract useful information, to a collector system. They can also keep records of packets matching access control lists. Whilst continuous logging of all traffic is recommended, often a specific access control list can be useful in answering a question. For instance, it would be possible to log all attempts to send email directly from client computers, in support of a policy that they should not do so.

Where a VPN (*Virtual Private Network*) is implemented in a router or firewall, the device can capture records of use, attempted use and authentication.

b. Email gateways

The University maintains two activity logs in this context - these are the Googlemail logs and a separate SMTP email gateway for internal traffic.

c. Googlemail logs

This is useful for tracking down a sender or recipient's missing messages, such as those that have been quarantined as spam or otherwise routed incorrectly. **Only super administrators have access to email log search.**

d. SMTP Logs

The SMTP gateway stores header information relating to system generated in-house email traffic (e.g. SupportWorks emails). The logs reveal source and destination information and subject line.

e. Proxy servers

Web proxies should log each URL with the time and the internal IP address requesting it, so that any request can be traced to its source.

f. Shared workstations

It is desirable that there is a record of who was logged in to any computer at any time. Typically the records will be generated by DHCP, login or RADIUS server.

g. Wireless Network Access

The AMP system records session data for all wireless connections across the University. Records are created for each user access. These records include: username, location data, connection time and connection speed.

3.0 How much activity should be logged?

3.1 It may be useful to age your log files gradually, so that you keep raw data close at hand for a short time in case of immediate operational need, and then archive it to another location in a standard format for long term storage.

4.0 Timestamps

4.1 NTP (*Network Time Protocol*) is the normal way to maintain accurate time on at least one server with an external connection; other internal devices may use NTP, SNTP or a proprietary protocol locally, perhaps referring to this single internal server, to keep their clocks correctly set.

5.0 Where will the logs be kept?

5.1 One or more dedicated logging servers should be established - to which computers and other network devices can send their log information.

5.2 Logging servers must be continuously available and they should run as few other services as possible, to reduce the risk to critical data from failures and vulnerabilities in applications.

5.3 Access to logged information (especially write access) must be carefully controlled, authenticated and audited, both in terms of the individuals authorised to use the data and of limiting the range of addresses from which the log servers are reachable.

5.4 Adequate backup arrangements for the logging servers must be in place.

6.0 Who can read the logs?

6.1 Read access to the logs should be limited to people in appropriate roles.

6.2 UK legislation specifies the notices and warrants which authorise or require you to release information, and you must insist on having such authority. You must also verify the identity of any officer or agency to whom you disclose information.

7.0 How long should logs be kept?

7.1 Janet CSIRT will not expect you to retain logs for more than three months, however, logs are generally kept for up to one year.

7.2 If log information is required as evidence, the chain of custody becomes very important. You may, for instance, be asked to demonstrate that the records you have made available could not have been altered.

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk