Internet and E-mail Usage

Procedures

Procedure Ownership	
Owner:	Head of Information Technology
Author:	Information Technology Staff Officer
Screening and Proofing	
Section 75 screened:	*18 November 2015*
Human Rights proofed:	*17 November 2015*
Consultation	
	Union consultation – October-November 2015
Approval	
SMT:	*3 November 2015*
Board:	*11 December 2015*
Version	
Version:	1.0
Publication date:	
Implementation date:	*11 December 2015*
Review date:	*No later than December 2019*

Document Control

Version No.	Date	Description
0.1	October-November 2015	Union Consultation
0.1	3 November 2015	Draft for approval by SMT
0.1	11 December 2015	Draft for approval by Board
1.0	11 December 2015	Approved by Board

Alternative Formats

This documentation can be made available in alternative formats such as large print, Braille, disk, audio tape or in an ethnic-minority language upon request. Requests for alternative formats can be made to the Probation Board using the following contact information:

Communications Department
Probation Board for Northern Ireland
80-90 North Street
Belfast
BT1 1LD

Telephone number: 028 90262400
Textphone: 028 90262490
Fax: 0300 1233290
E-mail: info@pbni.gsi.gov.uk

Contents

1. Aim

The aim of this document is to define the Probation Board for Northern Ireland's (PBNI) procedures on internet and e-mail usage. The procedures apply to all electronic devices capable of using the internet and email. The procedures apply to all PBNI staff and Board members.

2. Internet Usage Policy Provisions

2.1 PBNI has software and systems in place that can monitor and record all Internet usage on PCs, laptops and tablets supplied by PBNI. These systems are capable of recording (for each and every user) each internet site visit, e-mail message and file transfer into and out of the internal networks.

2.2 Logs of such traffic are held for three years. PBNI reserves the right to (i) monitor and record internet and e-mail usage at any time and (ii) inspect any, and all, files stored in any areas of its networks in order to assure compliance with its policies. PBNI will review internet and e-mail activity and analyse usage patterns, and may publish the overall activities and patterns of PBNI.

2.3 Unless expressly identified and recorded for a business need, e.g. in connection with policy on sexual offences, the display of any kind of sexual image or document on any PBNI system is a violation of PBNI policy on sexual harassment. This type of material may not be accessed, archived, stored, distributed, edited or recorded using the PBNI network or computing resources.

2.4 PBNI Internet facilities and computing resources must not be used to violate laws and regulations applicable in the United Kingdom. Any software or files downloaded via the Internet into PBNI networks become the property of PBNI. Any such files or software may only be used in ways that are consistent with their licences or copyrights. PBNI retains the copyright to any material posted on the Internet by any employee in the course of his or her duties.

2.5 Staff may, subject to written local management approval, participate in officially sanctioned newsgroups or chat rooms in the course of business relevant to their duties. When so doing, staff must not (unless specifically authorised to do so) speak or write in PBNI's name and must make it clear that your participation is as an individual speaking only for you. Staff must identify themselves honestly, accurately and completely. Staff must refrain from political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service.

2.6 Online social networking can be a useful business tool and, although the potential benefits are great, use of these technologies inherently carries greater risks than traditional web browsing. These risks largely come from the fact that the content of online social networks is predominantly user-generated. Damaging and/or inappropriate content can also be published and disseminated easily. These risks threaten the Confidentiality, Integrity and Availability of the data on the PBNI network. However, the risks are not solely related to Information Assurance. Online social networking usage could potentially also undermine personnel safety, organisational reputation and the safety of the public who interact with an entity via these services and could lead to complaints or breaches of the Code of Conduct.

2.7 PBNI uses firewalls to assure the safety and security of its internal networks. Staff must not attempt to disable, defeat or circumvent any PBNI security facility.

3. Responsibilities

3.1 STAFF MAY

3.1.1 Use PBNI internet and e-mail facilities for reasonable personal use. This can be defined as:

a) use outside of core time;

b) use during official breaks;

c) use at any other time at management discretion;

d) use which does not breach specified guidelines in the policy regarding web based facilities (e.g. use of chat rooms is not permitted, use of social networking sites is not permitted);

e) use for any purpose which does not breach the conditions set out in any other policy or guidance documentation.

3.1.2 Make occasional use of the Internet for on-line banking or the purchase of goods and services for example books, flights, CDs and so on provided payment is made by the individual, delivery of items purchased is to a private address, and you order the goods using a personal e-mail address.

a) Users must not create any unauthorised contractual liability on the part of PBNI.

b) PBNI does not accept (i) any responsibility for the security of credit card details, or any other payment method used, or (ii) any liability for losses or other liabilities arising out of transactions, whether as a result of fraud or howsoever caused, suffered while using PBNI systems for personal transactions. All such use is entirely at the individual's own risk.

3.2 STAFF MUST

3.2.1 Respect copyrights, software licensing rules and property rights, download only software with direct business use and do so in accordance with departmental policy.

3.2.2 Keep all user IDs and passwords secure as staff are responsible for all activities recorded under them. User passwords help maintain individual accountability for Internet resource usage and provide protection for individuals against fraud and misuse.

3.2.3 Be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of your account. Impersonation or unauthorised use of another user's identification will be considered a breach of security.

3.2.4 Identify themselves honestly, accurately and completely (including your position in PBNI and your function, when requested) when setting up accounts on outside computer systems e.g. discussion groups.

3.2.5 Give due regard to maintaining the clarity, consistency and integrity of PBNI's corporate image and avoid making any inferences that may prove inappropriate from a PBNI perspective.

3.3 STAFF MUST NOT

3.3.1 Reveal protectively marked information, personal data, client data, or any other material covered by departmental policies and procedures.

3.3.2 Knowingly connect to any internet site that contains inappropriate material. If staff accidentally connect to such a site, they must disconnect from that site immediately regardless of whether that site was previously deemed acceptable by any screening or rating programme. Staff should report any such events to the PBNI Information Technology Security Officer (ITSO) immediately as a safeguard in the event of a subsequent investigation.

3.3.3 Use PBNI internet or e-mail facilities to carry out activities for personal gain including for example share dealing or monitoring, investment portfolio management or gambling.

3.3.4 Use internet facilities, CD-ROM or e-mail to download entertainment software such as music, screensavers, games, or to play games over the Internet.

3.3.5 Download videos unless there is an express work related use for the material, noted and approved by line management.

3.3.6 Upload any software licensed to the PBNI or data owned by the PBNI without the express authorisation of the Information Asset Owner (IAO).

3.3.7 Use the PBNI internet facilities to download any virus or programme designed to infiltrate a system to gather information (eg worm, Trojan Horse) or other type of malicious program code.

3.3.8 Use the PBNI internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

3.3.9 Use the PBNI internet facilities to connect to, or use, social networking sites (*a website, which allows individuals to construct a public or semi-public online profile and to connect with others who share similar interests and views*) such as Facebook, Twitter, etc unless authorised by PBNI for work purposes.

3.3.10 Use the PBNI internet facilities to connect to, or use, third party e-mail provision sites such as hotmail, gmail, yahoomail, etc.

3.3.11 Use PBNI facilities to run a private business e.g. freelance or consultancy work.

3.3.12 If staff misuse the internet in any of the ways described above, they may be subject to disciplinary action. In certain circumstances this may be regarded as gross misconduct and could result in dismissal.

4. E-mail Code of Conduct

4.1 Users should apply similar standards to the use of e-mail as other carriers of information such as the telephone, fax and the postal system. However, some special precautions are needed. For example e-mail is often spontaneous and can be written and issued without spending much time thinking about the content.

4.2 E-mail also allows large amounts of information to be distributed very quickly and irretrievably. Therefore care and consideration needs to be given to the content of e-mail messages. In particular staff should guard against:

a) writing messages that could be interpreted as disparaging, offensive, inflammatory, libellous or harassing; and

b) passing on such messages to other staff

c) protectively marked information which is contained within the content of long e-mail chains.

4.3 As in the case of external or internal mail sent to the wrong person, it is the staff member's responsibility to ensure that e-mail received in error is properly re-directed or returned to the originator. In addition, if a staff member is the accidental recipient of Protectively Marked material or personal data, they must also report the incident to the ITSO. If staff receive what they consider to be an inappropriate internal e-mail, they should forward a brief note to the sender explaining that they do not wish to receive any further e-mails of that nature. If the sending of inappropriate e-mails continues, staff should advise their line manager as a safeguard in the event of any subsequent investigation.

4.4 If staff receive an inappropriate e-mail from outside PBNI which falls into the category of "spam" (unwanted and unsolicited e-mails sent to multiple e-mail addresses) they should not respond to the e-mail but notify the IT Helpdesk.

4.5 Staff may make occasional use of e-mail accounts to send brief personal e-mails subject to the conditions for using e-mail set out in this policy. Personal documents should only be stored temporarily on PBNI systems. Personal e-mails must be clearly marked 'personal'. It is an explicit condition of using this facility that staff accept that the content of such e-mails may be accessed by the ITSO, management and/or IT support staff, without notice or any requirement for further consent.

4.6 While it is not intended to undertake routine monitoring of the content of e-mails (personal or otherwise), e-mail traffic may be accessed at any time either as a result of checking an officer's e-mail account for business reasons if they are absent from work, or as part of an exercise to monitor compliance with the Internet and E-mail Usage policy. Staff must not use PBNI official templates and the following disclaimer should be added to the foot of the message:

"This e-mail is a personal communication and is not authorised by or sent on behalf of PBNI"

4.7 Staff must not use the e-mail system to send or store sexual or offensive material. If staff receive any such inappropriate material via e-mail they must report the incident to the ITSO immediately.

4.8 Staff must not promote or participate in “chain mail”. Chain mail is when you are asked to send a particular message to a number of other people who are also asked to send it on. These messages commonly promise good luck, success or help for charitable causes. They are designed to be annoying and/or damaging, and they slow down computer systems. Staff should delete any such mail immediately upon receipt.

4.9 Staff must not send OFFICIAL SENSITIVE e-mails or e-mails with OFFICIAL SENSITIVE attachments to internet e-mail addresses e.g. gmail, yahoo etc. This includes your own home e-mail address.

4.10 Staff should not forward personal e-mail from a home account to their PBNI e-mail address. If staff have completed work at home, which has been authorised and is not protectively marked, it may be forwarded to their PBNI e-mail address.

4.11 Staff must remember to use the Out of Office Assistant within Microsoft Outlook to inform customers and colleagues that you are unavailable. If away unexpectedly, line managers may contact the IT Helpdesk to activate the Out of Office Assistant with an appropriate message.

5. E-mail Security

5.1 The PBNI corporate system is linked to GSi which enables staff to send protectively marked data up to and including OFFICIAL SENSITIVE data to other government departments also linked to GSi. OFFICIAL SENSITIVE data can also be sent to CJSM e-mail addresses.

5.2 Some other systems may be connected to the GSi; staff should consult the ITSO for confirmation.

5.3 E-mail can be sent to organisations with an OFFICIAL protective marking without OFFICIAL in the header/footer.

5.4 If staff are transmitting protectively marked information, they must ensure the e-mail contains the correct Protective Marking label at the top of the covering e-mail and all attachments are correctly labelled.

6. Storing E-mails

To enable compliance with a wide range of statutory duties and responsibilities, PBNI has a duty to keep a permanent record of all significant documents. At present, this means that a paper copy of any important or significant e-mail, with or without attachments, which constitutes a record, must be made and filed. A paper copy is needed where the e-mail message contains material which:

- provides the only evidence of the origin of and/or date of receipt of an attached document which needs to be retained;

- records decisions or provides authority for action;

- will be needed to maintain business continuity;

- might be needed for administrative, accounting, audit, research or historical purposes;

- might be needed to prove whether an activity or transaction took place; and/or

- could be requested under the Data Protection or Freedom of Information provisions.

7. Non Compliance

7.1 Failure to manage information in accordance with relevant PBNI policies (procedures or guidance) and appropriate legislation may result in disciplinary and/or criminal action. Line management must report any breach, or suspected breach, of policy to the ITSO. The circumstances will be investigated initially by line management and **cases will be subject to normal disciplinary procedures. In certain circumstances a breach of this policy may be regarded as gross misconduct and lead to dismissal.**

7.2 The following are some examples of what will be regarded as a breach of this policy and subject to disciplinary action. The list is not exhaustive but is representative of areas or issues that staff should be especially vigilant about:

- deliberate access of pornographic, sexual, inappropriate or offensive material

- over-use of personal e-mail

- inappropriate site visited and line manager/ITSO not informed

- using the internet to obtain software for personal use e.g. screen savers or games;

- subscribing to private sector mailing lists via PBNI for purposes other than those that are work-related

- generating messages in a way that makes it appear they came from someone else

- sending messages which are abusive, offensive, libellous or a nuisance

- generating and/or distributing chain e-mail

- using IT facilities for political or commercial activity

- disseminating or printing copyright material in violation of copyright laws

- contravening rules for personal use of IT facilities

- contravening PBNI IT or other security policies.

7.3 In some circumstances, misuse of e-mail may constitute not only a disciplinary offence but also a criminal one.

7.4 Staff should be aware that the possession of child pornography is a criminal offence. PBNI will fully co-operate with law enforcement authorities to identify and take action against any member of staff accessing, possessing or disseminating such material. Individuals found to have been involved in any way in the possession or dissemination of child pornography using PBNI information systems may face serious disciplinary action with a high probability of dismissal irrespective of whether or not they are prosecuted or convicted under the criminal law.

7.6 Staff should note that they may be personally liable to prosecution, and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim that you had not intended to harass or cause offence may not in itself constitute an acceptable defence.

7.7 Unless expressly identified and recorded for a business need, the use of ICT facilities to disseminate inappropriate material which could cause offence to others (irrespective of whether any offence is intended) may constitute harassment and will not be tolerated. Inappropriate material may include, but is not limited to, any material of a pornographic, homophobic, sexist, racist, sectarian, violent or offensive nature or that uses disablist language, whether in pictures, cartoons, words, sounds, or moving images, and whether or not purporting to be of a humorous nature.

7.8 Further advice and guidance on the policy can be sought from the personnel listed in the 'Contacts' section of this document.

8. Internet and E-Mail Monitoring

Monitoring of employees in PBNI is carried out within legislative requirements and is carried out to balance the rights of staff to privacy and personal data protection against PBNI's duty to ensure that:

- Staff can work in a safe and harmonious work environment;
- Staff do not breach national security guidelines;
- Staff do not engage in criminal activity;
- Staff do not engage in activities likely to bring the reputation of PBNI into question;
- Staff do not otherwise abuse their conditions of employment.

The management of monitoring in PBNI is the responsibility of the Director of Probation who has delegated the daily monitoring of electronic communications to the Information Technology Security Officer (ITSO) and the IT Department.

Monitoring of internet and e-mail is carried out using automated checking software to:

- find out whether staff are sending or receiving inappropriate e-mails;

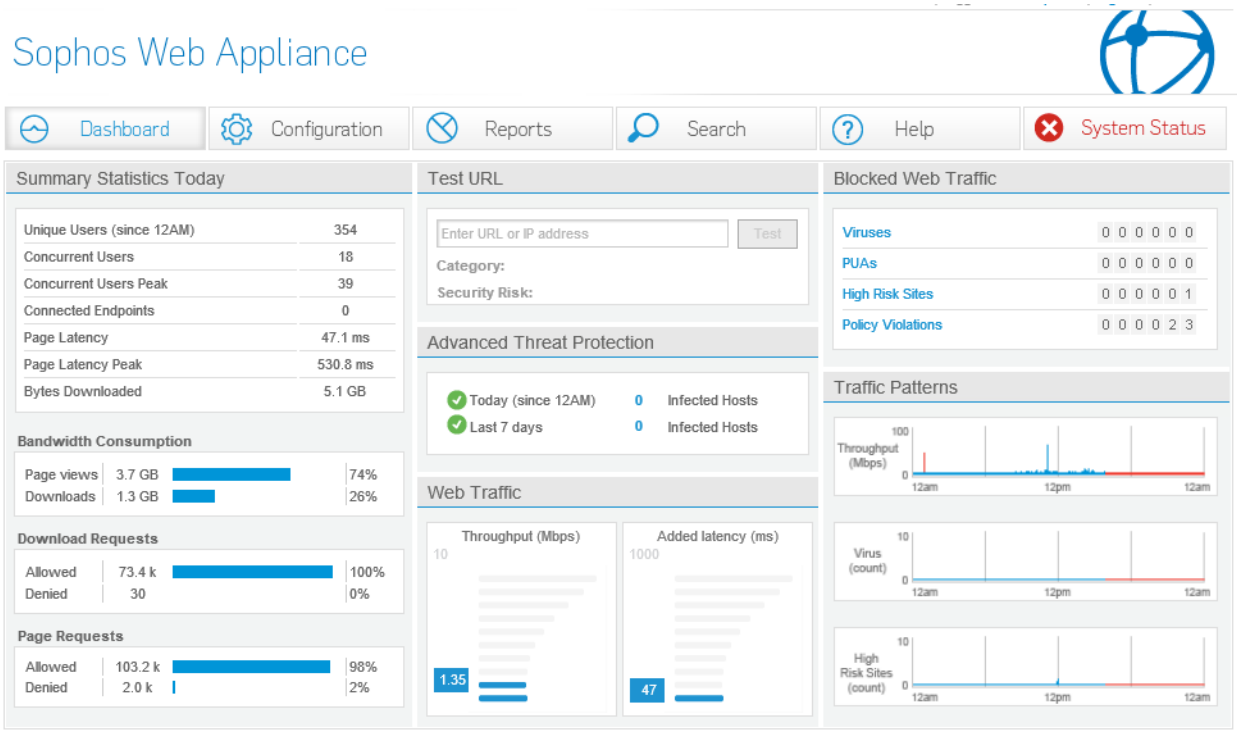
- monitor and archive all outbound e-mail for any potential security leak so that evidence can be investigated;
- examine logs of websites visited to check that staff are not downloading pornography or information of a criminal nature or that will seriously affect the reputation of PBNI.

Although the monitoring processes are automated, the final assessment of the results will require human interpretation and action, managed by the ITSO.

The devices used for internet and e-mail monitoring are Sophos WS1100 and ES1100 embedded appliances.

8.1. Internet Monitoring

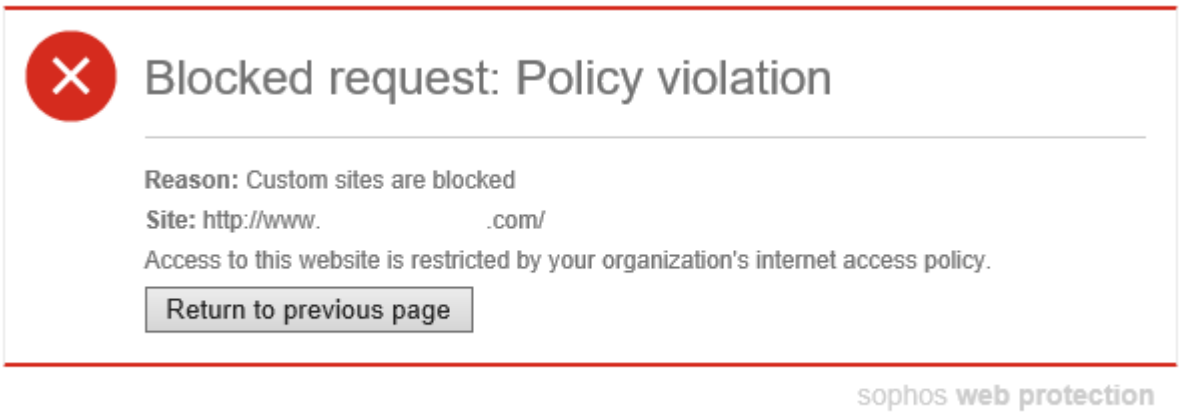
Monitoring of the internet is carried out by the Sophos WS1100 web appliance.



Any website browsed from the PBNI domain is automatically recorded by the Sophos WS1100 appliance.

If the sites are deemed to pose no threat or risk (as per pre-defined lists of 'safe' sites) they are automatically approved and the user is forwarded on to the original content.

If the site is deemed to be a threat (e.g. Adult Material, General Webmail, Social Networking sites etc.) then the user is automatically notified via a browser screen - as shown below – that the site is 'blocked' and this information is recorded in the logs.



The web filter logs are checked on a scheduled basis twice a day – once at 11 am and again at 5 pm.

They are also checked ad-hoc if an automatic e-mail warning is sent to the Helpdesk by the Sophos web appliance.

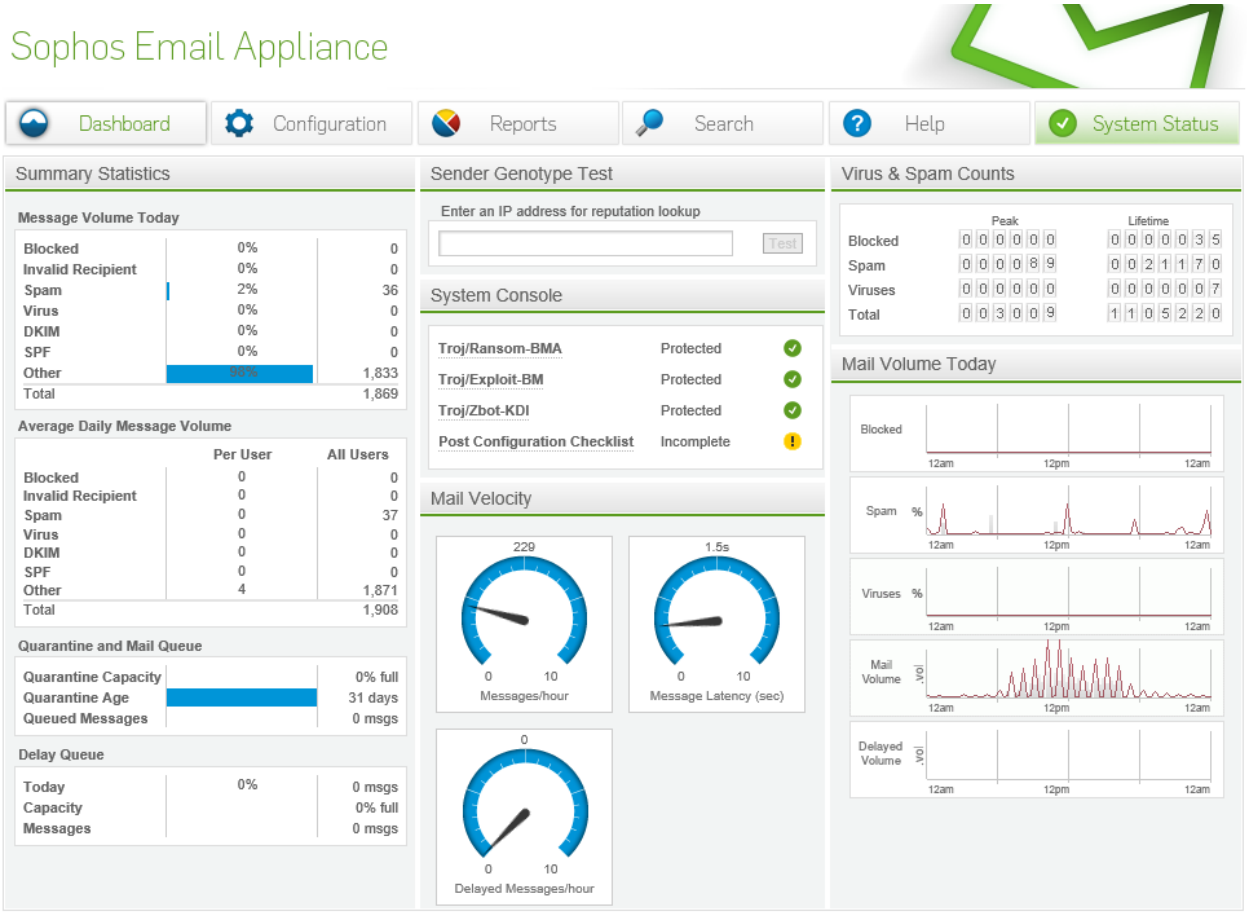
If an automatic e-mail is sent to the Helpdesk or, through the scheduled/ad-hoc checks of the web filter logs, a 'blocked' site is discovered, these details are checked for the following information:

- A single visit to a website.
- The actual 'type' of website visited (is it actually 'adult' or simply contains details that would be classed as 'adult' but may be necessary/valid in terms of Probation work – such as sexual offence details).
- Trend of websites visited by user.

If any of the above checks are deemed to be of a serious nature, the details are brought to the attention of the ITSO who will instigate a formal 'Incident', following the 'Incident Response Plan' procedures. In the absence of the ITSO the details will be brought to the attention of the Head of Information Technology.

8.2. E-mail Monitoring

Monitoring on the e-mail system is carried out via a Sophos ES1100 embedded appliance.



All e-mails coming into, or going out of, the PBNI domain, are automatically scanned by the Sophos appliance and the To and From addresses logged, along with the subject line.

The Sophos ES1100 appliance scans e-mails in 2 ways:

1. by e-mail address/domain (ie @domain)
2. by keyword

Addresses/domains can be whitelisted, which simply means to automatically allow passage to the recipient, no matter the content/keywords of the e-mail or blacklisted, which simply means to deny passage, no matter the content/keywords of the e-mail.

Keyword filtering assigns a numerical score to certain words and, when a threshold is reached, blocks the e-mail from being sent/received.

Examples of keywords that are scanned for, and a score assigned, are:

- racist terms
- sexual words
- offensive/abusive terms
- expletives
- common spam (Rolex, Viagra etc.)

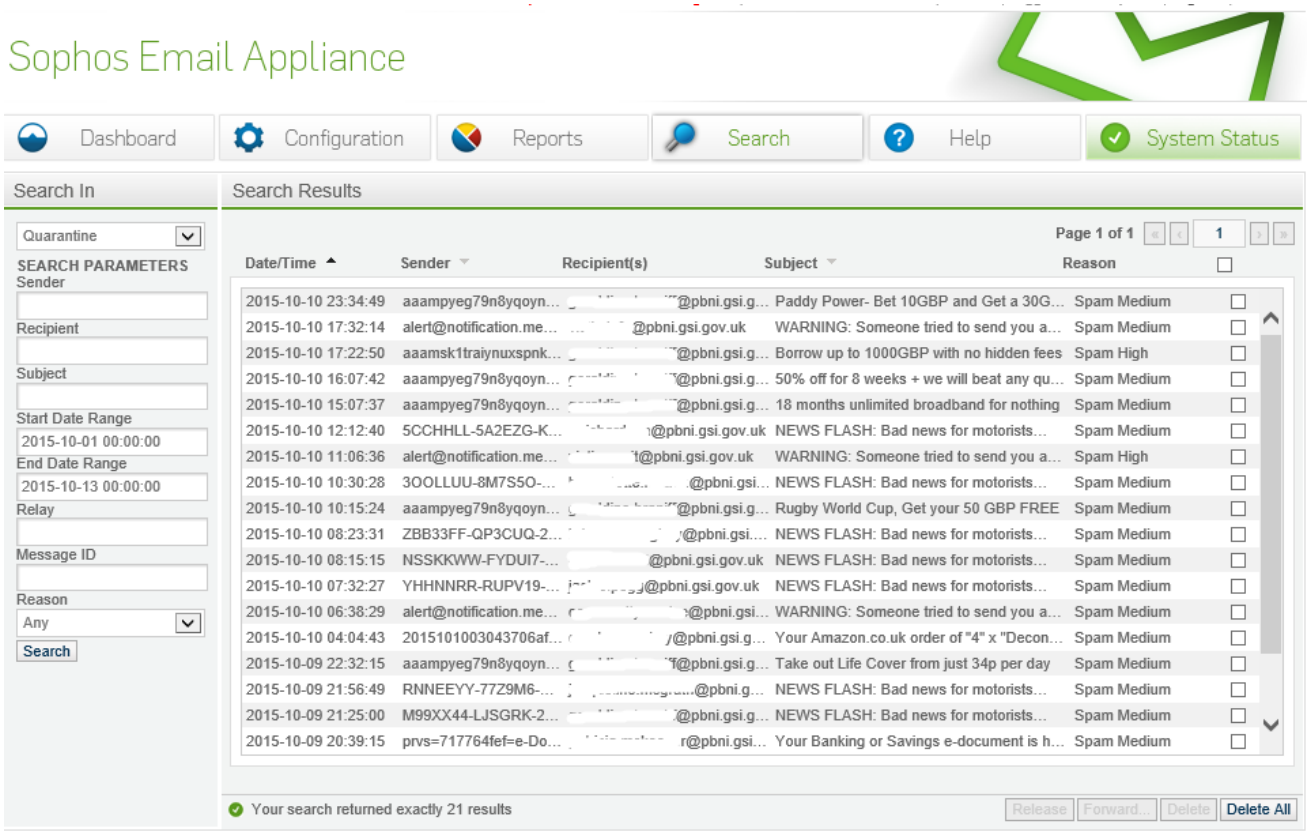
- PBNI defined words

If e-mails are deemed to pose no threat they are automatically forwarded to the original recipient where they will be received via Outlook (internally).

For valid business reasons some addresses/domains are not checked for content/keywords. For example the work of sex offender management necessitates sexual words/offensive/abusive terms to be used. In the case where regular communication takes place between PBNI and an approved partner agency (such as PSNI) a whitelist can be created to ensure that e-mails are not delayed unnecessarily no matter the keywords used/threshold reached.

If e-mails are deemed to be a threat (spam, blended threat, contains keywords etc) they are automatically quarantined and require manual intervention to determine further action: release to recipient, deletion (in the case of spam) or manual intervention to confirm content is appropriate and authorised.

The quarantine list is checked on a scheduled basis four times a day – 9 am, 11.30 am, 3 pm and 5.30 pm. It is also checked, on an ad-hoc basis, throughout the day.



In the case of an outgoing e-mail being blocked the sender is notified, for an inbound e-mail, the intended recipient is notified by e-mail immediately, stating the reason that the message was blocked and advising the user to contact the Helpdesk for assistance.

If a member of staff, after receiving such an e-mail, contacts the Helpdesk or, through the scheduled/ad-hoc checks of the quarantine list, a 'blocked' e-mail is discovered these details are checked for the following information:

- The sender/recipient address
- The content/nature of the e-mail
- The nature/threshold leading to quarantine

If these checks determine that the e-mail can easily be classified as of being of 'no threat' then it will be manually released; if it is classified as being 'spam' then it will be deleted. If, however, further manual intervention is required to confirm content is appropriate and authorised the e-mail will be placed into the 'Pending' section and brought to the attention of the ITSO.

The ITSO will perform an initial investigation to decide if the e-mail should be released; this may involve contacting the recipient or, in some cases, a manager, to determine the nature of the e-mail and appropriate action.

If any of the above checks result in the e-mail being deemed to be of a serious nature, the ITSO will instigate a formal 'Incident', following the 'Incident Response Plan' procedures.

In the absence of the ITSO, the details will be brought to the attention of the Head of Information Technology.

9. Reporting

The Sophos ES1100 e-mail appliance gives overview information such as:

- Amount of throughput of e-mails
- Types of e-mails quarantined
- Keywords used
- Thresholds

If required a formal report can be manually put together to detail any of the above. In the case of a quarantined e-mail leading to a formal 'Incident Response' being necessitate this, of course, will lead to a fully documented report.

The Sophos WS1100 web appliance has the facility to run numerous, standard reports such as:

- Virus downloads
- High risk sites
- Policy violations
- Top bandwidth users
- Users by browse time
- Browse summary by users
- Top users by site category
- Site visits by user
- User search queries

For each of these reports it is possible to drill down to detail a specific user's web activity on a specific date and time, as well as analysing browsing trends, duration etc.

The Sophos WS1100 web appliance also caters for the creation of business defined, ad-hoc reports tailored to any criteria that the system collects.

These reports can be run from a single moment in time viewpoint, across a date range, for a single user, for a single URL/domain/website or across many different subject areas.

On a monthly basis standard reports can be produced and sent to the Head of Information Technology and the Head of Human Resources.

For example:

- Top 10 sites visited
- Users exceeding 30 hours online
- Top 10 blocked sites
- Top 10 users visiting blocked sites

On request any ad-hoc, business defined reports can be produced for the senior managers.

A line manager may request a browsing activity report on a member of their staff by completion of a Browsing Activity Request Form (see Annex A). The form must be completed in its entirety and include the reason why the report has been requested. This should include discussion with the relevant senior manager and, if appropriate, HR Department (e.g. if staff member is a Union representative). Unless there is a valid reason for not doing so, the staff member should be informed that the request has been made. Completed forms should be sent to the ITSO. The maximum period for which a report can be requested is for the previous 6 months.

Managers should note that if a report is provided which subsequently results in disciplinary action, a copy of the report must be supplied to the person to which the report relates.

10. Contacts, Enquiries and Advice

If you require any further information on these procedures, you should contact:

TITLE	EMAIL / PHONE
IT Security Officer (ITSO)	infosec@pbni.gsi.gov.uk 02890 262516
IT Helpdesk	helpdesk@pbni.gsi.gov.uk 02890 262432

Annex A

BROWSING ACTIVITY REQUEST FORM

Name:
Grade:
Location:
Period of Report:
Reason for requesting report:
Line Manager Name:
Grade:
Location:
Date:

Note: If as a result of providing the requested report, a disciplinary case ensues, a copy of the report must be provided to the individual at the outset of the disciplinary case.