1 SPIRE Security Reminders for Exporters – Individuals and Companies

1.1 Potential Exporters - Individual Users

Before using the SPIRE system you must read and understand the SPIRE (BIS) Password Policy, Security Policy and guidance on the SPIRE Login Page. These will tell you how to create an export application and how to access your information on the SPIRE system.

You must keep your password a secret in order to make sure that no-one else accesses your information.

The SPIRE Password and Security Policies are available respectively at

https://www.spire.bis.gov.uk/eng/fox/espire/password_policy

and

https://www.spire.bis.gov.uk/eng/fox/espire/security_policy

You must report all suspected SPIRE security incidents to the SPIRE Helpdesk at eco.spire@bis.gsi.gov.uk.

There are five other things that you must do to protect your computer and hence your information on the SPIRE system. These are as follows:

1. Install anti-virus software ("AV")

"Viruses", "worms" and "Trojans" are collectively known as malicious software or just "viruses". They are a constant threat to any system connected to the Internet. Malicious software can infiltrate you computer without you knowing and can create havoc.

Viruses can be stopped by ensuring that your PC has AV software running on it and that the AV software is kept up-to-date.

2. Install a personal firewall

A firewall detects any unexpected incoming connections from the Internet or unexpected outgoing connections to the Internet. These connections may be used to send information from your PC without you knowing. They may be the result of malicious software that has found its way onto your PC e.g. by clicking on an attachment in an email.

Firewalls that protect against both unexpected incoming connections from the Internet and unexpected outgoing connections to the Internet will need to be "trained" in what is to be allowed and hence need more effort to set up.

3. Install antispyware

Spyware and other unwanted software might find its way onto your PC and lead to unwanted pop-ups, slow performance, and leakage of information from your PC.

4. Keep your software up-to-date

This includes your operating system and any other programs you have installed on your PC. You should set this up to work automatically e.g. in Microsoft Automatic Updates. It will repair any faulty software that might be exploited by malicious software.

5. Keep your hardware secure

If others can gain physical access to your computer they might install a software or hardware keystroke logger that could provide them with your username and password details. Only allow trusted persons access to your computer. This applies to your children's friends and computer repair shops!

If you are using Microsoft Windows™ XP or Vista on your PC then you can use the firewall which comes with these systems. If you do not have AV software, a firewall or antispyware, then you can either buy a commercial product or download one from the Internet. You should choose a product that provides automatic updates and set it up accordingly.

Note: products downloaded from the Internet may be only for individual users and not for commercial use.

1.2 Potential Exporters - Company Users

Before using the SPIRE system you must read and understand the SPIRE (BIS) Password Policy, Security Policy and guidance on the SPIRE Login Page. These will tell you how to create an export application and how to access your information on the SPIRE system.

You must keep your password a secret in order to make sure that no-one else accesses your information.

The SPIRE Password and Security Policies are available respectively at

https://www.spire.bis.gov.uk/eng/fox/espire/password_policy

and

https://www.spire.bis.gov.uk/eng/fox/espire/security_policy

In order to protect your information you must follow any instructions given to you by your SPIRE Company System Administrator.

You must report all suspected SPIRE breaches and incidents to your SPIRE Company System Administrator.

1.3 Potential Exporter - Company System Administrators

Before setting up and making use of the SPIRE system you must read and understand the SPIRE Company System Administrator Guide provided by BIS Company Registration guide at:

https://www.spire.bis.gov.uk/docs/CompanyRegistration.pdf.

This will tell you how to set up access to SPIRE and how to work in a secure way.

You must act as the central point for your users to report suspected security incidents. You must report all suspected SPIRE security incidents to the SPIRE Helpdesk at eco.spire@bis.gsi.gov.uk.

You must make sure that the workstations used by SPIRE Users are secure.

To protect your Company computers and your information on the SPIRE system you must:

1. Install anti-virus software (“AV”), a personal/host firewall, and antispyware on any workstation that is used to access SPIRE.

2. Keep your software up-to-date. This includes your operating system and any other programs are installed on your workstations. You should set this up to work automatically e.g. in Microsoft Automatic Updates.

3. Keep your hardware secure. If others can gain physical access to your workstations they might install a software or hardware keystroke logger that could provide them with your username and password details. Beware of any cameras that could record passwords being entered.

When using SPIRE you, and your company users, must log in as a normal workstation user and not as an administrator.

Unprivileged users and processes must not be able to disable or reconfigure the Personal Firewall software. The personal firewall should implement a default deny policy and should only allow those services that are explicitly required.

Support for macros on workstations must be disabled unless there is a valid business case for their use.

Any data to be introduced through removable media should be virus checked by one, preferably two functionally different virus checkers. This includes USB ‘sticks’.

Disable Automatic preview of e-mails unless there is a valid business case.