CySPAG Registered Installer Scheme

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association

Contents

1. Introduction

The objective of this scheme is to allow installation organisations to be recognised as responsible installers, and maintainers of connected products.

The requirements listed in this document (see Annex A) have been identified by CySPAG as the minimum acceptable cyber security measures, related to the installation and maintenance of connected safety and security products.

For an Installation organisation to be recognised as a CySPAG Registered Installer, they will need to declare in writing that they have the necessary Policy and Procedures in place to meet the Scheme requirements and that they commit to following these Policy and Procedures.

2. Policy and Procedures

CySPAG has prepared a default set of policies and procedures (as listed in Annex A, the 10-point plan and outlined in Annex B manufacturer compliance and system updates, to meet the requirements of this scheme).

CySPAG recommends the Installation organisation adopt these Policies and Procedures.

Alternatively, the installation organisation may create their own policies and procedures which should be written in a way to ensure compliance with the Scheme (Annex A).

3. How to achieve and maintain Registered status

The Installation organisation will need to submit Annex C of this form, along with the registration fee as indicated on the CySPAG website at URL: www.cyspag.co.uk/fees

If accepted, the installation organisation will be listed on the CySPAG website and granted use of the CySPAG **Registered** Installer logo.

To retain permission to use the logo and maintain the listing on the CySPAG website, the installation organisations will need to be re-submit Annex C on an annual basis.

4. Annex A – CySPAG Registered scheme requirements

The Installation organisation shall be able to demonstrate that they have policies and procedures in place to ensure that the Installation organisation shall:

1) Install devices and applications from CySPAG registered manufacturers. If the manufacturer is not CySPAG registered, The Installation organisation will perform due diligence by confirming that the manufacturer:

   a) Supplies advice and support about installing products securely.

   b) Communicates information about security updates, critical updates, and withdrawal of update support.

   c) Supplies advice and support for how to implement security updates.

   d) Has a vulnerability disclosure policy which includes how to report vulnerabilities.

   If the items listed above cannot be fulfilled the installation organisation should not use the product from the manufacturer

2) Install devices and applications securely and in accordance with the manufacturer's recommendations. Where this is not possible or unclear, the Installation organisation will seek guidance from the manufacturer or supplier or relevant stakeholders e.g., those responsible for the network.

3) Ensure where the hardware and software components of the system are provided by others, The Installation organisation will confirm and document who has responsibility for cyber security e.g., a PC, router, or switch supplied by the client.

4) Ensure the security of the network that the devices and applications are connected to is not compromised by the installation.

5) Check and apply as required any security updates to all installed devices, applications, and system(s) during both installation and maintenance activities.

6) Offer the client a maintenance schedule and if accepted, inform them about security updates/support. Where there is no warranty/maintenance schedule in place, the installation organisation will inform the client that they are not responsible for security updates/support.

7) Subscribe to receive and/or monitor manufacturers information on security updates and security update support.

8) Apply the security updates in a timely manner e.g., at the next scheduled maintenance visit.

9) Agree appropriate action with the client to apply the critical security updates as soon as possible.

10) Inform the client if the manufacturer withdraws security update support for an installed device or application and inform the client that no further updates can be supplied, which may reduce the protection against vulnerabilities/exploits and advise the client on appropriate options.

5. Annex B – Policy and procedures for an installation company complying with CySPAG Registered

Note: where the words [Installation company] are listed below, these should be replaced by the name of the Installation Organisation adopting these Policies and Procedures.

Manufacturer compliance

[Installation company] will ensure that, where available the devices and applications installed by [installation company] are from CySPAG registered manufacturers.

If the manufacturer is not CySPAG registered, [Installation company] will perform due diligence by confirming and recording for each manufacturer of the equipment:

a) How to get advice and support about installing products securely.

b) How to get information about security updates, critical updates, and withdrawal of update support.

c) How to get advice and support for how to implement security updates.

d) How to access the manufacturers vulnerability disclosure policy, and how to report vulnerabilities.

If the manufacturer is unable to provide information on all items, [Installation company] will not use the product, and will source product(s) from another manufacturer.

Any equipment adopted due to alarm system 'take overs' shall be deemed as installed by [installation company] and this policy applies.

Security updates and Security update support

[Installation company] subscribes to receive and/or monitors manufacturers information on security updates and security update support by the following methods:

- For manufacturer A – Signed up to notifications at [insert manufacturers web page as appropriate]
- For manufacturer B – Check the monthly newsletters, and/or any additional emails.
- For manufacturer C – Check the manufacturers website regularly to see if there has been any updates/change at [insert manufacturers web page as appropriate]

Note: The methods listed above are for example purposes only, and the Installation company should list their own approach for each manufacturer of devices and applications installed by the installation company.

[Installation company] will inform the client if the manufacturer withdraws security update support or notify of the intention to withdraw security update support for an installed device, application, and or system(s):

- Inform the client that no further updates will be supplied, which may potentially lead to vulnerabilities and exploits, and that the risk will increase overtime.
- Advise the client on appropriate mitigation such as disconnecting the equipment from the internet, and/or replace the equipment.

Note: Mitigations should be undertaken in line with the notification period.

Secure installation

[Installation company] shall install devices and applications securely and in accordance with the manufacturer's recommendations. Where this is not possible or unclear, [Installation company] shall seek guidance from the manufacturer or supplier or relevant stakeholders e.g., those responsible for the network. If guidance is not available, then the equipment shall not be added to the network.

[Installation company] shall not perform any amendments to the security of the network unless the change has been recorded as authorised by client.

During installation of devices, applications, and system(s),[Installation company] shall check and apply as required any security updates to all installed devices, applications, and system(s).

Maintenance of devices and applications

During maintenance activities of devices, applications, and system(s), [Installation company] shall check and apply as required any security updates to all installed devices, applications, and system(s).

Security Updates – non-critical **–** [Installation company] shall apply updates to all installed devices, applications, and system(s) within **12** months from release of a non-critical security update or at the next scheduled maintenance visit (whichever occurs first).

Security Updates – Critical – [Installation company] shall agree appropriate action with the client in order apply updates to all installed devices, applications, and system(s) upon release of a critical security update to ensure the update is applied as soon as practicable.

Support

[Installation company] shall offer the client a maintenance schedule. If this is not accepted, [Installation company] shall inform the client in writing:

a) there is no warranty/maintenance schedule in place.

b) that [Installation company] are not responsible for security updates/support.

c) to disconnect the installed devices, applications, or system(s) from the internet or any other networks.

Where a maintenance schedule is in place, but the client refuses to grant access, [Installation company] shall inform the client that the risk of vulnerabilities and exploits may increase if maintenance activities, are not performed as per the maintenance schedule.

6. Annex C – declaration of commitment for a CySPAG Registered Installer

Installation organisations name:	
Installation organisations registered address:	
Primary contact name:	
Primary contact email address:	

I declare that:

- I am a duly authorised member of the installation organisation e.g., Business owner or Director.
- The policies and procedures that relate to the CySPAG Registered scheme requirements submitted to CySPAG have been integrated into our business practices.
- Our installation organisation commits to following the policies and procedures submitted to CySPAG.

This commitment remains valid for a period of 12-months from the date of acceptance by CySPAG (from the original acceptance date if this is an update during a current declaration period) or until this declaration is superseded by an updated declaration, or until the declaration is withdrawn.

Name of duly authorised person making this declaration:	
Role within the Installation organisation:	
Date signed:	

CYSPAG use only

This declaration has been accepted as being accurate by CySPAG.

CySPAG person name:	
CySPAG person signature:	
Date accepted:	

Note 1: More information can be found in form 342 issue 1, and at URL: https://www.cyspag.co.uk/copy-of-registered-companies or email at: info@cspag.co.uk.

Note 2: CySPAG is a trading name fully owned and operated by the BSIA Ltd.

Disclaimer: *The 10 points specified serve as guidelines for best cybersecurity practices related to installing and maintaining connected safety and security products. CySPAG assumes no liability for any security issues or breaches arising from implementing these practices.*

About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.