The following provides guidance for applicants of the Licence Management service for the completion of a Code of Connection.

Note: this is only relevant to businesses applying for, or using, our Licence Management service.

Code of Connection between *[insert name of company]* and the

Security Industry Authority

Address

Tel number

Statement of commitment

I confirm that the code of connection is accurately completed and has been authorised by the following:

Director (or other competent person within the business) Authorisation

Signature

Role: *e.g. Chief Information Security Officer*

SIA Authorisation

SIRO /DSO

Signature ……

Purpose

Licence Management eligibility criterion 1.3.2 requires the business must confirm its ability to meet data security, storage and transmission standards as specified in our (SIA) Code of Connection.

The Code of Connection gives us a level of assurance that your systems (approved contractor) which access and use our information and systems are managed and controlled to acceptable levels.

We expect to have in place security controls on your systems that meet the requirements of *Cyber Essentials Plus*. You are required to provide evidence (valid certificate) that you have undergone a successful *Cyber Essentials Plus* evaluation as part of your application to use the Licence Management service.

Certification to ISO27001:2013 is an acceptable alternative to *Cyber Essentials Plus* provided that licence management operations come within the scope of that certification.

Note: accredited out sourced IT is not acceptable.

You must be able to provide us evidence of assurance when we request it.

Requirement

You require access to our portal in order to add, amend, submit and view records relating to your applications for SIA licences. You will use HTTPS protocols and approved user names and passwords to authenticate to the portal.

The following table provides example compliance statements and additional guidance against each element of the Code of Connection. The purpose is to assist you in your completion of the self-assessment. They are not additional requirements but indicate the type of information and level of detail that should be included in your self-assessment.

You are strongly advised to access the Cyber Essentials website hosted by the National Cyber Security Centre and view the technical requirements documentation on that site.

For ease of reference, for each element of the Code of Connection we have provided the relevant *Cyber Essentials* requirement.

Note:

- We have the right to audit your company and your security controls at any time which could involve a site visit from a member of our security team.
- We have the right to upgrade these requirements at any time according to the specific threat status and advances in technology and recognised standard.

Inspection/assessment

Our Senior Information and Risk Officer (SIRO) reviews and signs off each business's Code of Connection through our information assurance group. Except where we have concerns, this is completed as a desk-top exercise, and 'sign-off' means that we are assured that the information security arrangements meet the licence management eligibility criteria.

	Description	Compliance Statement	Guidance
CoCo-1	Information security, acceptable use, access control, audit, logging, anti-virus and patching policies or standards are in place and documented.	*The company is fully compliant with Cyber Essentials Plus and has an Information Security Policy that includes the policies identified. Certification against Cyber Essentials Plus has been independently verified. All parts of CoCo1 are covered within the scope of our CE Plus certification which is maintained throughout the year by IT security, IT management and internal assurance functions.*	Apart from the relevant certificate for Cyber Essentials Plus, or ISO27001:2013, there is no need to submit relevant documentation except where specifically requested by the SIA.
CoCo-2	All hosts and network equipment are located in secure accommodation, which is commensurate with protecting information assets appropriately.	*The company has a 24-hour physical security presence which is backed up by a third party intruder and fire alarm system. The company has a door access system which operates through the use of staff passes and a no pass back mechanism is incorporated across the company. The company is compliant with Cyber Essentials Plus and has separate enclosures for information storage systems. Server rooms have separate door access controls and authorisations from the rest of the company.*	Cyber Essentials Plus – Access

CoCo-3	An acceptable use policy is in place and users positively confirm their acceptance to all policies.	*The company has acceptable use and information security policies as attached. All staff are mandated to complete yearly awareness courses on data protection.*	
CoCo-4	All local, remote attached devices and network infrastructure supporting devices are security hardened	*All devices, including mobile devices connecting into the company's infrastructure are hardened to company standards. No unhardened devices connect to the infrastructure. All elements of CoCo 4 are covered and independently tested within the CE Plus certification. Where personal devices are connected to the infrastructure under a BYOD policy their use has been subject to independent testing as part of the CE Plus certification.*	Cyber Essentials Plus – Secure Configuration
CoCo-5	The minimum security standards applicable to the approved contractor, using the licence management service, shall be certification against Cyber Essentials Plus.	*The company uses CE Plus as its security baseline in meeting information security objectives and is further independently assessed and accredited to hold personal data and information defined as sensitive under UK data protection legislation.*	Cyber Essentials Plus
CoCo-6	Only information requested shall be introduced to the SIA portal.	*Only required information will be introduced to the portal through authorised personnel who will hold the required authentication details.*	Cyber Essentials Plus - Boundary Firewalls & Internet Gateways
CoCo-7	The systems used to connect to the SIA portal are protected by either a hardware or software firewall, or antivirus applications with regular daily updates.	*The company incorporates firewalls and antivirus across all of its systems. These are maintained and updated on a daily basis and users do not have access to change any of the settings.*	Cyber Essentials Plus – Malware Protection
CoCo-8	The systems used to connect to the SIA portal will not run any automation applications or macros against the portal.	*All users with authorised access to the portal are aware of their obligations concerning inputting data onto the SIA portal. All authorised staff are aware that the running of any automation software or macros on SIA portal is prohibited.*	Cyber Essentials Plus – Secure Configuration

CoCo-9	The systems used to connect to the SIA portal is subject to an operating system and application patching regime.	*The company's systems are mandated to operate in accordance with the companies patch management policy (as attached).*	Cyber Essentials Plus – Patch Management
CoCo-10	The systems used to connect to the SIA portal will be operated and supported within the EU.	*All authorised personnel who are required to input information into the SIA portal will all be based in an office located within the UK. No information will be input into the SIA portal outside of Europe*	
CoCo-11	Incidents, which may lead to the compromise of the SIA data, will be reported to the SIA without undue delay but in any event no later than 24 hours upon becoming aware.	*The company's incident management process incorporates clear escalation procedures that comply with the requirements of the Data Protection Act 2018. All incidents including near misses which may lead to a compromise of SIA data will be notified to the appropriate SIA contact.*	