

Preamble:

The aim of this document is to provide an overview of the Continuing Professional Development (CPD) requirements.

CPD is mandatory for those registered on the Professional Register of cyber security professionals, held by the UK Cyber Security Council.

The requirements will be flowed down through the license with the licensee. There is an expectation that licensees of the Council mandate CPD among the cyber security practitioners within their members.

Demonstration of commitment to CPD is an integral and mandatory part of the competency requirements for all cyber security practitioners irrespective of role or specialism.

INDEX

- Introduction
- The Council CPD Policy Statement
- Summary of requirements
 - Licensees
 - Registered Professional Practitioners
- CPD Criteria for licensed bodies
- Monitoring of CPD records for professionally registered individuals

1. Introduction

1.1. It is vital that professionals remain competent and, therefore, are required to demonstrate that their knowledge (Competence A) and professional skills (Competences B-E) are being kept current. This is particularly important because of the continual advances and growth in cyber and cyber security. This growth means that there is an increasing need to understand the changes and implement advances as they are identified, developed, and become mainstream. This is particularly important whether considering the system as a whole or interfacing with other disciplines providing non-functional requirements. It requires the individual to develop and maintain up-to-date knowledge and skills to ensure they can meet the needs of the evolving professional requirements.

- 1.2. The Council acknowledges that it is the responsibility of individuals to ensure the systematic maintenance, improvement and broadening of knowledge and skills, in turn to ensuring continuing competence throughout their career; that is to say, it is the responsibility of individuals to undertake CPD.
- 1.3. All successful applicants who become professionally registered, through assessment and recommendation by any licensed member of the Council, commit to maintaining and enhancing their competence by undertaking CPD. It will be a requirement that the individuals maintain membership of a licensed professional body to support their CPD.
- 1.4. CPD has several purposes, which will vary in relation to the individual's own circumstances, needs and career progression. It can also take a variety of forms.
- 1.5. At its core is experiential learning through the challenges and opportunities of working life. This is supplemented by interaction with others such as colleagues, customers and suppliers, and professionals from other disciplines - all leading to enhanced competence.
- 1.6. It may also be supplemented by structured activities such as courses, distance learning programmes, private study, preparation of papers and presentations, mentoring, involvement in professional body activities, or relevant voluntary work. The list is not exhaustive and individual registrants are best placed to determine their own development needs and how to meet them.
- 1.7. There may also be requirements from the employer; a particular qualification or from the licensee of which the individual is a member. Existing professional bodies often promote the planning of structured CPD that incorporates a balance of sources including training, work experience, academic study, volunteering, events/seminars, and self-study.
- 1.8. CPD records prepared for other purposes may also be acceptable evidence of CPD. Examples include records produced for other professional institutions/organisations, company training, development, and appraisal processes.
- 1.9. One of the core purposes of the Council is the development and professionalisation of the cyber security profession. As such, the Council

promotes and supports the professional development of its registrants.

1.10. Organisations licensed by the Council are committed to support their members CPD in several ways.

2. UK Cyber Security Council CPD Policy Statement

- 2.1. CPD is accepted across most professions as ‘the systematic acquisition of knowledge and skills, and the development of personal qualities, to maintain and enhance professional competence’. Regardless of their registered status, all individual members of organisations licensed by the Council have a mandatory obligation to maintain their competence through CPD, and to support the learning of the wider community. Council professionally registered individuals must commit to the planning, recording, and making available for reporting of their own CPD.
- 2.2. This obligation underpins the value of the professional titles¹ of the cyber security profession, as well as enabling society to have confidence in the profession.
- 2.3. Employers or experienced colleagues will often play a significant part in this process, but individuals should be responsible and proactive in planning and in seeking professional development opportunities.
- 2.4. While it is expected that cyber security professionals will undertake CPD on a regular, on-going basis, it’s accepted that some activities may occur without deliberate planning or recording of activities such as in the workplace as part of their everyday role.
- 2.5. Whatever its purpose or nature, learning through CPD should be reflective and should, where possible, relate to specific objectives even if these are only to maintain their professional cyber security competence. Having a regularly reviewed development plan will facilitate learning, although there will always be a place for unplanned activities. Recording and reflection on activities, and the outcomes they have had in terms of individual learning, is a valuable process for turning learning into competence.

¹ The specific professional registration titles are the subject of a separate document.

- 2.6. The Council expects that a documented CPD record is a requirement of maintaining Professional Registration. The Council further expects that this record is submitted (in a suitable format) for monitoring as required by the Licensee of which the registrant is a member.
- 2.7. In line with accepted good practice, the CPD activity must be related and relevant to the specialism of the registered professional, resulting in maintained or enhanced knowledge and skills.
- 2.8. The Council requires licensees to 3-yearly monitor, which may include sampling of members CPD records to assure compliance. Licensees will be required to demonstrate that they provide both appropriate support and guidance for members' CPD.

3. Summary of Requirements

3.1. Licensees:

All bodies licensed by the Council will:

- a. meet the requirements and criteria set by the Council.
- b. support registered individuals with their CPD and promote good practice.
- c. mandate CPD for their members and monitor compliance of registered individuals, and
- d. implement suitable sanctions for non-compliance of registered individuals.

3.2. Registered Professional Practitioners

All individuals registered on the UK Cyber Security Council Professional Register, are expected to:

- a. display a commitment to CPD,
- b. plan and record their CPD in line with the competence requirements of their current organisation membership, qualification and employment, and
- c. adhere to the policy.
- d. Undertake a minimum of 25 hours of CPD per year across several sources, totalling 75 hours of the three years

- 3.3. Registrants who are temporarily 'not in active practice' may request a temporary exemption from the requirements to submit a record of their CPD. It is for the membership body to agree any waiver of the CPD reporting requirement and the individual will therefore be exempt from an audit during this period. Upon

return to “professional activity” the registrant will be subject to the normal CPD reporting requirements.

4. CPD Criteria for licensed bodies

- 4.1. Any organisation licensed by the Council shall have a CPD policy and auditing process as outlined below that is compliant with this CPD Policy.
- 4.2. The Licensee policy shall:
 - a. mandate CPD recording of registered members’ CPD records,
 - b. enable the registered professional to show continuous and ongoing development in terms of their discipline and career, demonstrating their ability to learn and reflect,
 - c. require the registered individual to record and reflect on their CPD as part of a continuous cycle of planned development.
- 4.3. In addition, licensees are expected to support their members through the following:
 - a. encouraging a positive and proactive approach to CPD;
 - b. recommending a structured approach to CPD that registered individuals may use to plan and record their CPD appropriately, but which also allows flexibility for those who may be supported by an employer or other scheme;
 - c. support registered individuals by providing, or signposting them towards, guidance, resources and support programmes, such as mentoring. These should be in line with current good practice, encouraging reflective practice to improve competence relevant to the registered individual’s role and area of practice; and
 - d. providing effective feedback.

5. Assessment for CPD

- 5.1. Individuals are expected to undertake at least 75 hours of CPD on a 3 yearly cycle, (25 per year) from a blend of sources.
- 5.2. The Licensee will be expected to audit the following percentage on registered individuals:

- a. 20% for the first License period; if positive outcomes;
- b. 10% for the next License period; if positive outcomes continue;
- c. 5% for the next License period from then onwards until the License is terminated for any reason.

5.3. A positive outcome will be that all those audited meet the minimum 25 hours required and that the CPD was relevant to the individual.

6. Monitoring of CPD records for professionally registered individuals

6.1. The Council's intention is to encourage a culture in which registered individuals will naturally engage in CPD and take ownership of their own learning and development. The Council believes that adopting this approach across the cyber security profession will help all registered individuals to plan and reflect on their own learning and development in a more conscious way, to their own benefit, to that of their employers, and of society.

6.2. Recording evidence of CPD undertaken is an important part of consciously planning and assimilating CPD and is therefore a requirement of professional registration. Licensee policies must include appropriate processes to sanction registered individuals who persistently fail to comply with the licensee's CPD policy.

6.3. This should include the risk of removal from membership, and consequently the Council Register and therefore the ability to continue to use the Council's titles and post nominals. The names of professionally registered individuals removed from the Register due to non-compliance with published CPD requirements will be made available to other Licensed Bodies, as necessary.