Chartered Institute of
Information Security

Guidance Notes for Fellowship

Version 2.0

Contents

1. Introduction

Fellow is the highest level of attainment in the Chartered Institute of Information Security's (CIISec) membership levels and is there to:

- Recognise industry leaders in the information/cyber security profession.
- Meet the aspirations for recognition of achievement and contribution to the profession, within the current membership body.
- Attract those in the profession with higher levels of skills, experience, respect and attainment.

1.1. Fellow Requirements

The requirements for individuals applying for consideration to become a CIISec Fellow are:

- Professional Leadership – demonstration of professional leadership factors within the information security industry
  - Eminence
  - Authority
  - Seniority
  - Contributions to the Profession
- Two supporting nominations from individuals with the following CIISec status
  - 2 x Fellows
  - 2 x Board members
  - 1 x Full Member nomination & 1 x Board member nomination
  - 1 x Full Member nomination & 1 x Fellow nomination
  - 1 x Board member nomination & 1 x Fellow nomination
- A current Curriculum Vitae (CV)
- An interview with peers.
- The conferring of Fellowship is subject to the applicant meeting standards of ethics as defined by CIISec.

2. Application Form

The information that you provide on your application form will be used and processed by CIISec and third parties for the purposes of processing your application.

To assist CIISec with its assessment of applicants, your information may be passed to appointed referees and volunteers (third parties). These third parties will only process your data as instructed by CIISec. Security measures have been taken to ensure your information is kept secure.

As outlined above, by submitting your information you consent to the processing and transfer of your data.

If you have any concerns about your information being processed in this manner, please contact accreditation@ciisec.org before proceeding with the submission of this form.

The information supplied in the application form will be retained for a period of 3 years post your award, after which time it will be deleted. Under no circumstances will the information you provide be used for marketing purposes.

3. Completing the Application Form

Applicants will need to complete a Fellow Application form detailing personal details, the nominations and reference details. Applicants must also submit a detailed CV.

The application form must be submitted to CIISec via the Secretariat by sending to accreditation@ciisec.org

The application form is made up of three parts:

PART 1 – Personal Details

PART 2 – Nomination and Referees

PART 3 – Declaration

3.1. Extraordinary Criteria Requirements

Applicants will be required to demonstrate that they surpass at least 3 out of the 4 of the areas. In order to validate they have the skills and experience for consideration as a CIISec Fellow, the applicant will need to do this by completing a short application form; provide their CV and take part in an interview. The applicant's CV should include details of work history and cover the extraordinary criteria requirements, which will be discussed in more detail during the interview. Note: The examples given in each area are illustrative, not definitive.

3.1.1. Eminence

An eminent individual will have general recognition and acknowledgement across all or part of the information/cyber security community. They should have wide knowledge or expertise in a particular field and have made a significant contribution to advancing the knowledge and understanding of that specialism. Normally an eminent individual would have a substantial and respected record of publication and public speaking. Examples of this may include:

- Having written several influential books within the sphere of information/cyber security.
- Authored a number of papers within a particular area of information/cyber security which advances that body of knowledge.
- Having given a number of public lectures on a defined information security topic.
- Media work (e.g. interviews or commentaries on cyber security issues or topics).
- Successful recognition as, for example, an expert witness, arbitrator or consultant.
- Interaction with senior government officials or ministers.
- Has a record of influencing cyber security development within industry sectors (e.g. Finance, Law Enforcement, etc.)
- Having been head-hunted to fill a senior role or invited to participate in national or international review bodies, boards or committees.
- Membership of National, International or Government Cyber Security Boards and Committees.

3.1.2. Authority

An authoritative individual is recognised and respected for their knowledge and expertise that may be in a particular specialism. This may be demonstrated by:

- Exercising authority over persons who are not directly under the applicant's control in the areas of security and organisational developments.
- Recognition as an authority on a certain aspect of cyber and information security. Examples may include a technical specialism (e.g. security architecture, audit, penetration testing or red teaming, incident investigation, forensics, legal and regulation, etc.) or within a specific business area (e.g. finance, utilities, oil and gas, nuclear, merchant marine, etc.)

- The development of a technique which has become widely used e.g. payment security or significant work for and involvement in, technical or professional security committees, such as national or international standards committees, or professional bodies.

3.1.3.Seniority

Within the seniority category an individual should be considered to be at a senior level where they possess relevant responsibility for an area. An individual should be able to demonstrate a clear career progression to this position and have held it for several years. Some examples may be:

- In charge of over 50 people of whom 50% should be at CIISec Full Membership standard (or equivalent); in higher education at a grade at least equivalent to Senior Lecturer teaching information/cyber security to degree level; or within a commercial training environment where they can demonstrate significant development of security related training programmes.
  In consultancy within an organisation or self-employed working for major clients at a senior or highly responsible level.

Seniority can be assessed on the basis of having risen to a senior cyber security role in an organisation; or by moving between organisations into more senior roles; or having set up an developed a company; or a combination of these.

3.1.4.Contribution to the Profession

Applicant's will need to demonstrate outstanding commitment to the profession or professionalism, such as significant contribution to CIISec, or other relevant bodies, establishing professional standards, influencing political, educational, legal or ethical considerations, encouraging individuals, especially young people, into the profession and developing them.

Examples may include: active involvement in setting cyber security apprenticeship standards, setting up or delivering schemes to encourage young people into the profession; working with schools to generate an interest in cyber security amongst the students; contribution to initiatives to encourage diversity within the profession; working with government, trade bodies or regulators to set cyber security policy or standards.

4. Summary of Fellow Criteria Requirements

To conclude, applicants will need to demonstrate that they meet the Core Criteria and Extraordinary criteria as explained in previous sections and will be assessed to ensure that they are able to meet the criteria as set out below:

Criteria	Fellow
Academic Qualification e.g. degree	All relevant graduate or post-graduate degrees taken into consideration
Professional Qualifications e.g. CISSP, CREST	No additional PQ's required
Industry Contribution evident	Should be able to demonstrate
Management or Academic Level and/or people under control or budget	Should be able to demonstrate
Industry/Society Achievement	Should be able to demonstrate
Referee corroboration of capability and experience	2 Nominations from CIISec Fellows or Board Directors
Interview	Required
Upholding Professionalism standards within their organisation	Should be able to demonstrate
Confirms personal pledge to uphold professional ethics	Required
Holds awards for services to Cyber Security (e.g. MBE)	Consider against Eminence and Contributions to the Profession

5. Completion of Application

5.1. Submit the Form

Please submit your completed application form to accreditation@ciisec.org

5.2. Payment

Once your application form has been received the current fee will be added to your profile and you will be notified when payment is due. Your application will not be processed until payment has been received.