Version of 15 February 2019

**▬▬▬▬▬▬▬▬▬▬▬**

# Guidance for IT related information to be provided as part of Application Form for Investment Firms under section “Information on the organisation”

Under Commission Implementing Regulation (EU) [2017/1945](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1945&qid=1532531698985&from=EN) of 19 June 2017 the CSSF has issued an Application Form following Annex I for Investment Firms to complete when applying for a license with the CSSF.

This guidance aims to provide further guidance as to which information to provide under section “Information on the organisation”, more precisely regarding the information requests laid down in Commission Delegated Regulation (EU) [2017/1943](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1943&qid=1532531698985&from=EN) of 14 July 2016 under Article 6, with regards to IT related elements.

We would like to point out that this guidance solely focusses on IT aspects to be communicated under Article 6, more specifically under:

* (c) (ii) the description of the resources (in particular human and technical) allocated to the various planned activities;
* (e) a list of the outsourced functions, services or activities (or those intended to be outsourced) and a list of the contracts concluded or foreseen with external providers and resources (in particular, human and technical, and the internal control system) allocated to the control of the outsourced functions, services or activities; in case these outsourcings are related to IT
* (g) a description of systems for monitoring the activities of the firm, including back–up systems, where available, and systems and risk controls where the firm wishes to engage in algorithmic trading and/or provide direct electronic access;
* (i) details on the systems for assessing and managing the risks of money laundering and terrorist financing;
* (j) business continuity plans, including systems and human resources (key personnel);

In order to facilitate the provision of the abovementioned information we provide you with the below form which we strongly encourage applicants to complete.

# Form for IT related information to be provided as part of Application Form for Investment Firms under section “Information on the organisation”

|  |  |
| --- | --- |
| Your internal reference:  *[insert your internal reference]* | *Reference of the administration:* |
|  |

#### Administrative information:

1. Legal name of the entity:

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Name of the authorised director(s)/manager(s) having reviewed and approved this document:

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Date of transmission to the competent authority:

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

#### IT Organisation and strategy:

1. Please provide a summarised description of the IT organisation (organisational chart, number of staff, key IT and information security roles and responsibilities) and the selected IT strategy (in-house or partial/full IT outsourcing).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. In case of outsourcing, please:

* Specify the outsourced IT activities and provide information about the external provider(s) (in particular: company name, belonging to the group of the entity seeking authorisation, location/address, supervision by a supervisory authority, support PFS).
* Specify which IT systems will remain in Luxembourg under your responsibility (i.e. not outsourced)
* Confirm that a contract and/or SLA is signed between both parties and that this contract/SLA is in line with best practices and addresses the following points/requirements:
  + description of services provided by your contractor,
  + description of your responsibilities and of your contractor,
  + integration of your needs in your contractor's BCP/DRP and backups arrangements,
  + conditions for revocation/termination of contract and transfer to another service provider or hand over to you,
  + management of the outsourcing relationship (e.g. regular reporting / meetings between your contractor and you, incident management process, KPI, etc.)
  + conditions for sub-contracting for your contractor (e.g. your prior authorisation)
  + data confidentiality and security
  + possibility for your internal and external auditors and for your supervisor (i.e. the CSSF) to perform an audit on site
* Specify who will be in charge of this outsourcing within the entity seeking authorisation.
* Describe the controls implemented to ensure the quality of service and compliance with applicable regulatory requirements.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please confirm that the entity seeking authorisation will be responsible and actively involved in the management of the access rights (for instance validation of access rights requests and periodic access recertification, in accordance with “need to know” and “least privilege” principles) as well as the change management process of IT systems (i.e. changes to the IT environment impacting the data of the entity should be approved by the entity).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please clarify if the accounting system is located in Luxembourg or abroad. In case the accounting system is located abroad, In order to mitigate the risk of not being able to independently draw up a balance sheet and a profit and loss account, please clarify whether a copy of the basic accounting documents (including in principle the general ledger and the journal) will be available in Luxembourg.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

#### Description of the IT systems:

1. Please specify the “business” IT systems supporting the “business” activities provided (e.g. software for fund administration, transfer agent, accounting of domiciled companies, reconciliation, portfolio management, customer relationship management, Intranet, Website – consultative or transactional) and the “support” IT systems used for the organisation and administration of the entity seeking authorisation (e.g. the internal accounting and CSSF reporting systems, e-mail servers, internal files servers and access management tools like Active Directory).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please provide a summarised table indicating, for each application system listed at point A above:

* a short description of the application
* indication if it contains confidential data (of which type)
* the vendor of the application (if not in-house developed)
* the primary (production) hosting location of the application,
* the secondary (disaster recovery) hosting location of the application,
* the entity in charge of the IT infrastructure
* the entity in charge of the IT operations
* the entity in charge of the IT application maintenance
* the entity responsible (owner) for the application (e.g. you, a group entity, a third party..)

|  |  |
| --- | --- |
| *Please Annex the table to this form.* | *Reserved for the administration* |
|  |

1. Please specify if the entity seeking authorisation plans to use mobile devices (e.g. smartphones, tablets). In case of such usage, the entity shall describe the tools (e.g. Mobile/Enterprise Device Management tools) used to securely connect and control (including remote wipe, passcode lock, etc.) the mobile devices and confirm its compliance with the CSSF Annual Reports 2012 (Chapter XI, section 2.4.), 2007 (Chapter VIII, section 2.1) and 2005, (Chapter VIII, section 2.2.1).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please specify what type of telephone line the entity seeking authorisation will use (i.e. classical PBAX or VoIP). In this case, the entity shall confirm its compliance with CSSF Annual Report 2013, Chapter XI, 2.3.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please describe whether the entity seeking authorisation will host and administer its IT systems (support and business) itself on its premises. If not, please provide information on the type of service (e.g. PaaS, SaaS, IaaS), the system’s location (with an external provider or a provider belonging to the same group as the entity, in Luxembourg or abroad), the system operator (in particular: company name, location/address, belonging to the group of the entity seeking authorisation, supervision by a supervisory authority, support PFS) and on any system sharing with other entities (belonging to the same group as the entity seeking authorisation or not).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. In case of sub-outsourcing, the entity seeking authorisation shall ensure that the principles stated in the previous section, related to outsourcing, are respected by the entity which is contractually responsible of the information systems management and has to ensure that the process is under full control. Please provide all evidence that the process is effectively under control.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

#### IT Logical security:

1. Please describe the measures aiming at protecting the data in transit, either as part of your internal communications (i.e. on the network which is exclusively under your control) or external communications (e.g. through the Internet or leased lines). In particular, please specify:

* The redundancy of the lines, to ensure the service continuity.
* The network communication protocols (e.g. IPSec, SSL), including the symmetric (e.g. AES) and asymmetric (e.g. RSA) encryption algorithms, and the size of the corresponding keys.
  + The controls in place to ensure that the implementation of the encryption technologies is not exposed to known vulnerabilities (e.g. SSL vulnerabilities like Heartbleed, Poodle, etc.).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. In case of remote access, please specify:

* The persons who will use the external connections (e.g. employees, IT support, other entities belonging to the same group, external providers). In case you plan to authorise employees to remotely access the systems, please specify the number of people, the systems that are remotely accessible (indicating if they contain confidential data or not), the business purpose of such access and shall confirm its compliance to the CSSF’s requirements stated in the Annual reports 2013 (chap. XI, section 2.7.) and 2007 (chap. VIII, section 2.1.).
* The technical means used to provide remote access (e.g. VPN, Citrix, etc.), the (strong) authentication methods used (e.g. tokens) and the security controls in place to prevent the data leakage (e.g. hard disk encryption, block of USB ports, block of copy/paste and printing, etc.).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please specify the implemented security measures to ensure data protection, including data leakage prevention and segregation of environments in case systems are shared.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please specify if data at rest is encrypted. Should data at rest be encrypted, please describe the encryption process providing the encryption protocol, the encryption algorithm and the key lengths. Please specify the location of these keys and of any potential copies (backups) as well as a list of persons having access to the encryption keys.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please describe the controls in place over access to the information systems used by the entity (e.g. respect of the “need to know” and “least privilege” principle, regular access recertification, opening/closure of communication lines, user authentication, intrusion detection, antivirus, logs).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. In case the entity seeking authorisation provides Front end applications to its clients (e.g. Website, mobile application), please describe the functionalities of the applications, the security measures related to the underlying infrastructure, as well as the security mechanisms in place for the clients’ connections.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please provide a summarised description of your patch management process.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

#### IT Physical security:

1. Please describe the physical security measures and controls (access controls and environmental security measures) in place at:
   * the offices of the entity
   * the IT room/data centre of the entity, or if applicable, the outsourced entity.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

#### Business Continuity:

1. Please describe the backup process (in particular: full or incremental, frequency, retention periods, location of the backups and access restriction to the backups). The entity seeking authorisation must confirm its compliance with the CSSF Annual report 2012 (chap. XI, section 2.7.).

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please specify the secondary office location in case of the activation of the BCP (Business Continuity Plan). The entity seeking authorisation must confirm its compliance or commit to comply with CSSF requirements stated in the CSSF Annual report 2013 (Chapter XI, section 2.5.1.). Please describe the DRP (Disaster Recovery Plan) strategy (i.e. secondary site or not) and the high availability measures implemented.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please confirm that the entity seeking authorisation has a permanent, direct and unconditional (read and write) access to the IT systems provided by outsourced entities that allows the entity to take its activities back in hand at any time.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |

1. Please confirm that the backup solution, BCP and DRP are in line with the entity’s requirements in terms of continuity.

|  |  |
| --- | --- |
| *[enter text]* | *Reserved for the administration* |
|  |