DUE DILIGENCE QUESTIONNAIRE REGARDING OPERATIONAL CONDITIONS OF CLEARING MEMBERS

(number 5, c) of OMIClear Instruction B02/214)

1. **Information Security Management System (ISMS):**

☐ Our ISMS is fully defined, with a full suite of mature security policies, processes and controls, having formal executive management endorsement

☐ Our ISMS is still maturing, with a partial suite of security policies, processes and controls

☐ Our ISMS is under construction

☐ Our ISMS is non-existent

Please indicate if OMIClear data and/or related processing systems are under the scope of your ISMS

Yes ☐ No ☐

Obs:

2. **Security audits:**

☐ Formal security audits are carried out by an independent External body no less frequently than annually

☐ Formal security audits are carried out by an independent External body no less frequently than every two years

☐ Formal security audits are carried out by Internal Audit no less frequently than annually

☐ No recent formal security Audits

Please indicate if OMIClear data and/or related processing systems are under the scope of your Audits

Yes ☐ No ☐

Obs:

3. **Staff screening and contract management:**

☐ Pre-hire background verification screening processes at least on staff that has access to more sensitive data. Security clauses are included in all contracts

☐ Pre-hire background verification screening processes at least on staff that has access to more sensitive data. Security clauses are included only on contracts with staff that has access to more sensitive data

☐ No formal pre-hire background verification screening processes. Security clauses are included only on contracts with staff that has access to more sensitive data

☐ No formal personnel screening processes and/or no security clauses in contracts

Please indicate if contracts with staff that have access to OMIClear's sensitive or critical information data include security clauses

Yes ☐ No ☐

Obs:

4. **Staff security training:**

☐ All staff are specifically trained in our organization security obligations and responsibilities according to their role, at least once a year

☐ All staff are trained in our organization security obligations and responsibilities, at least once a year

☐ Staff security training processes are appropriate and effective, but the scope and frequency varies

☐ No formal staff security training is in place

Please indicate if your organization's security training include staff that have access to OMIClear's sensitive or critical information data

Yes ☐ No ☐

Obs:

5. **Identity and access management and control:**

☐ Formal admission/change/removal control requirements and mechanisms to ensure the appropriate privileges are routinely provisioned/de-provisioned across all systems are in place

☐ Formal admission/change/removal control requirements and mechanisms to ensure the appropriate privileges are routinely provisioned/de-provisioned across some systems selected on a risk/criticality basis are in place

☐ Non formal admission/change/removal control requirements: identity and access management is managed in an effective but ad-hoc manner

Please indicate if your organization's identity and access management control requirements and mechanisms include all applications used to process or store OMIClear's sensitive or critical information data

Yes ☐ No ☐

Obs:

6. **Access rights authorisation:**

☐ All user accounts are unique and rights are provisioned either based on formal authorisation of the relevant owner of each asset or based on the defined roles for every user/job type

☐ Some user accounts are shared accounts but rights are provisioned based on formal authorisation of the relevant owner of each asset

☐ All user accounts are unique but rights are provisioned on an informal basis

☐ Some user accounts are shared and rights are provisioned on an informal basis

Please indicate if any shared accounts are used to access applications used to process or store OMIClear's sensitive or critical information data:

Yes ☐ No ☐

Obs:

7. **Physical security:**

☐ Security perimeters are defined and used to protect all areas that contain or process sensitive or critical information. Physical access to those areas is restricted to specifically authorised personnel

☐ Security perimeters are defined and used to protect some areas that contain or process sensitive or critical information. Physical access to those secure areas is restricted to specifically authorised personnel

☐ No security perimeters are defined and used to protect the areas that contain or process sensitive or critical information. Physical access to those areas is not restricted

Please indicate if physical access to all areas that contain or process OMIClear's sensitive or critical information is restricted to specifically authorised personnel

Yes ☐ No ☐

Obs:

8. Handling of information:

☐ Sensitive or critical data downloaded, copied and/or printed from our applications is protected and stored securely. DLP, Classification and Handling and Disposal and Destruction controls to strictly control access, usage, transfer and destruction of data stored on devices are in place

☐ Sensitive or critical data downloaded, copied and/or printed from our applications is protected and stored securely. DLP, Classification and Handling and Disposal and Destruction controls are limited or do not exist

☐ Sensitive or critical data downloaded, copied and/or printed from our applications is protected in a limited way. No DLP, Classification and Handling and Disposal and Destruction controls are currently in place

Please indicate if sensitive or critical data downloaded, copied and/or printed from OMIClear applications is protected and stored securely

Yes ☐ No ☐

Please indicate if DLP, Classification and Handling and Disposal and Destruction controls to protect OMIClear's sensitive or critical information data stored on devices are in place

Yes ☐ No ☐

Obs:

9. Third party management:

☐ Critical or high importance third party service providers are subject to a security risk evaluation before onboarding and on a risk aligned periodic basis thereafter

☐ Critical or high importance third party service providers are subject to a security risk evaluation before onboarding and monitored on a periodic basis thereafter

☐ Critical or high importance third party service providers are subject to a security risk evaluation on an ad-hoc/risk related basis

☐ Critical or high importance third party service providers are not subject to security risk evaluations but are monitored on a periodic basis

Please indicate if all third party service providers (if any) that have access to OMIClear's sensitive or critical information data are subject to periodic security risk evaluations

Yes ☐ No ☐ Not applicable ☐

Obs:

10. Security incident management:

☐ Security incident management process documented (including roles and responsibilities, communication plan, evidence collection), forensics capability available and incident response testing executed no less frequently than annually

☐ Security incident management process documented, forensics capability available and incident response testing executed no less frequently than every two years

☐ Security incident management process documented and incident response testing executed no less frequently than every two years

☐ Ad-hoc security incident management arrangements in place

Please indicate if OMIClear's sensitive or critical information data related incidents are under the scope of your incident management process

Yes ☐ No ☐

Obs: