Information Security Guidelines for the Diligent Security System Project

1. Passwords shall be used that are difficult to guess, in accordance with Internal Procedure 10.20.3, 'User Identification Code, and Managing Password Array', clause 6.
   1. The password must be difficult to guess. The following rules shall be defined and enforced by the company's technical systems:
      1. The password must contain at least 8 characters.
      2. The password must contain alphanumeric characters.
      3. The password must contain at least one letter and one digit.
      4. The password may not include keyboard sequences (e.g., qwerty or poiuy).
      5. The password must not be based on the username or other identifying details of the user (identification code, names of family members, birth dates, etc.) such that the password can be easily guessed.
      6. It is recommended that passwords not consist of actual words to avoid the password being discovered by applying mechanized tools that identify words in the dictionary.
   2. The password set by the user is confidential and personal. It may not be transferred or made known to anyone. The password must not be recorded in a discernible place.
   3. The password will be valid for a limited period of time, and for no longer than 90 days.
   4. The user may change the password at any time that it becomes necessary or if the user suspects that the password has been discovered.
   5. A password may not be the same as any of the previous five or more passwords. Likewise, the user will not be permitted to change a password more than twice a day.
   6. After the fifth incorrect attempt at typing the password, the user will be blocked.
   7. In any event, if there is any suspicion that the password has become known, it must be reported to Information Security and the password must be changed immediately.
2. Authorized representatives will be appointed on behalf of the Information Security Department and they will have authorization to manage users (via access to OneClick Admin Site), change policies, and receive notifications of information security incidents/breaches of information security.
3. Authorized devices will be managed by Information Security representatives and not the supplier’s support representatives.
4. An idle session will be disconnected automatically once 15 minutes have passed.
5. The 2FA identification mechanism will be activated by using the supplier's application for both laptops and for PC software.
6. The management software of the system will be installed on the server/protected position (can be with Citrix).
7. Offline access to the system will not be permitted:
   1. Offline entrance to the system will not be permitted.
   2. The data protection key will be deleted from the laptop immediately upon disconnecting from the network.
8. Printing and exporting documents from the system will not be permitted.
9. A watermark will be embedded on the screens and will include the following items:
   1. Date and time
   2. Level of document's classification
   3. Username
   4. Name of document
10. The following types of documents may be uploaded: doc, docx, xls, xlsx, ppt, pptx, pdf, txt, jpg.
11. Users will not be permitted to enter the system via Touch/Face identification.
12. All traffic between clients and the supplier's servers will be encoded in the Communication Protocol TLS 1.2 with encoding algorithms AES 256 bit.
13. The supplier's servers must be protected and monitored by information security products such as Firewall, reverse proxy, anti-virus, anti-malware, IDS/IPS, and so on.
14. The supplier is obliged to ensure regular and secure back-up, and to perform hot backup, including updated DR and BCP programs.
15. The supplier must conduct regular applicative system risk surveys and permeability tests, and deal with any security breach that arises during a check.
16. The supplier must ensure the information is comprehensive, accessibile and available.
17. The supplier must provide complete separation of its clients' information.
18. The supplier will not be able to access clients’ information.
19. The supplier must manage a detailed log of users' activities (audit trail), that will be accessible to the client's system manager. This log will be secured and protected from alteration.
20. In all communications between the client and the supplier, the supplier will ensure that client's representative is authorized to deal with the matter at hand and the supplier will demand approved and signed documentation for any requests for changes in the system.
21. The supplier's software products will abide by the following requirements:
    1. The software code will be scrambled.
    2. SSL Certificate Pinning will be used.
    3. A mechanism for identifying breaches of cellular devices, such as rooting or jailbroken, will be used. Working with breached devices is completely prohibited.
    4. Information saved locally will be encoded with the algorithm AES 256bit.
    5. The mechanism will include control over types of documents that can be uploaded to the system.
22. The supplier's web products will abide by the following requirements:
    1. The ability to disconnect a user who is inactive for a defined period.
    2. Use of Cookies will be protected.
    3. Cache will not be used.
    4. Parameters requested to the server will be encoded so that their history cannot be overtly viewed.
    5. Users' identification will be performed by a token authentication combined with a nonce.