Appendix 2 – DCC's Security Specific requirements

1. Successful Tenderer should be responsible for patching application, database and third party components.
2. Application should be designed with Security and Privacy by Design principles.
3. Application and components must be kept up to date at all times.
4. Application should be compliant with OWASP top 10.
5. User access must be developed using Roles and Privilege Management principles.
6. Any data should be encrypted at rest and in Transit.
7. Any integration must be delivered using encrypted APIs.
8. Application segregation: Separation of presentation, business logic and database.
9. A Detailed solution document showing network design diagrams and TCP ports used between components must be provided and kept up to date.
10. Successful tenderer must have in place internal security and governance frameworks and/or standards (e.g. ISO27001) to ensure the appropriate delivery of required services in a secure manner.
11. Support personnel must access the system only using managed devices with up to date software and OS, Anti-Virus and Ideally EDR (End point detection and response).

END OF DOCUMENT