GUIDELINES

Secure System Guidelines (in respect of the obligation on Organisations to deploy and operate a Secure System)

1. Put in place (and thereafter monitor and enforce) the following procedures to prevent any loss, disclosure, or unauthorised use of any Private Key of any employees, contractors, partners, principals, directors or officers ("Individuals") within your Organisation:

1.1 System Access Control Procedures which (i) restrict access to information, (ii) prevent unauthorised access to information systems, (iii) ensure protection of networked services, (iv) prevent unauthorised computer access, (v) detect unauthorised activities, and (vi) ensure information security when using mobile computing and tele-networking facilities;

1.2 System Development and Maintenance Procedures which (i) ensure security is built in to operational systems, and (ii) maintain the security of application system software and data;

1.3 Physical and Environmental Security Procedures which (i) prevent unauthorised access, damage and interference to business premises and information, and (ii) prevent compromise or theft of information and information processing facilities;

1.4 Compliance Procedures which (i) are aimed at avoiding breaches of statutory, regulatory or contractual obligations and of any security requirements, and (ii) ensure compliance of systems with organisation security policies and standards;

1.5 Personnel Security Procedures that ensure that persons employed or affiliated your Organisation are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;

1.6 Organisation Security Procedures which (i) are aimed at managing information security within your Organisation, (ii) maintain the security of the information processing facilities and information assets of your Organisation which can be accessed by third parties, and (iii) maintain security of information when responsibility for information processing has been outsourced to a third party;

1.7 Computer and Network Management Procedures which (i) ensure correct and secure operation of information processing facilities, (ii) protect the integrity of software and information, and (iii) ensure safeguarding of information in networks and the protection of the supporting infrastructure; and

1.8 Security Policy Procedures that demonstrate management direction and support for information security through a documented security policy.

2. Ensure that all Private Keys being used within your Organisation (including without limitation by Individuals) as part of the Unipass Service are neither copied (except for back-up purposes) nor distributed.

3. Ensure that any copies of Certificates made for back-up purposes are subject to the same levels of protection applicable to original Certificates (including but not limited to protection by use of passwords).

Trusted Role Requirements (in respect of the obligation on Organisations to ensure that employees, partners, principals, directors or officers ("Staff") who wish to act as "Unipass Controllers" comply with these requirements)

1. The member of Staff must be a responsible and experienced individual within your Organisation who is capable of acting with due care and skill.

2. The member of Staff must be a trustworthy and competent individual who is capable of (i) keeping accurate records of all applications by other members of Staff and/or contractors of your Organisation ("Individuals") for Certificates, (ii) verifying and validating the details within Certificate applications and (iii) notifying our Registration Authority promptly when he or she receives a request from Individuals that their Certificate be revoked.

3. The member of Staff has never been the subject of a disciplinary action or proceedings (except in connection with petty misdemeanours) during the course of his or her employment with your Organisation.

4. The member of Staff has not been convicted of any crimes (except minor traffic offences) and is not subject to any criminal charges or investigations.

Unipass Guidelines (to be followed by Unipass Controllers)

1. Obtain authority from your contract signatory to represent your Organisation and/or "Associated Company" or "Network Member" * (if applicable) in the role of Unipass Controller.

2. When notified of applications for Unipass Certificates from members, employees, directors, officers, partners, principals, or contractors of your Organisation and/or its Associated Companies or its Network Members ("Individuals"), validate them following the rules in the table below to confirm:
    a. The applicant's employment or membership (or similar affiliation) with your Organisation and/or its Associated Companies or Network Members.
    b. The applicant's identity as described in the application.
    c. The integrity of all other information provided in the application.

Validation Requirement	Rules
Postal address confirmation	Check that any branch postcode supplied is valid for both the applicant and your Organisation or the Associated Company.
Personal investigation	Check the following: 1) Applicant is an Individual within your Organisation, Associated Company or Network Member (ie member, employee, director, officer, partner, principal, or contractor). 2) Applicant has a legitimate requirement to hold a Certificate on behalf of your Organisation, Associated Company or Network Member. 3) Applicant fulfils the role specified in the application.
Third-party confirmation	Check the following: 1) Appropriate organisational procedures have been followed to ascertain that the Individual is a legitimate member of your Organisation or the Associated Company (such as the Personnel or Human Resources department of your Organisation, Associated Company or Network Member taking up references for employment or membership (as applicable), or seeking appropriate indemnities for contractors).

3. You must NOT approve an application for further processing by the Unipass Helpdesk unless the application has been successfully validated by you. If you are unsure about any stage of the validation process please contact the Unipass Helpdesk for assistance (by sending an email to customerservices@origo.com.
4. Promptly request the revocation of a Certificate for an Individual whenever:
    a. any of the information within the Certificate contains, is known or is suspected to be inaccurate or could reasonably be believed to have been compromised;
    b. there has been a loss, theft, modification, disclosure or other compromise of the Private Key of the Certificate;
    c. any activation data, such as a password or PIN, used to protect the Private Key of the Certificate is compromised or suspected to have been compromised;
    d. there is a change in the identity of your Organisation, Associated Company or Network Member (e.g. through merger or acquisition, or change of name of your Organisation, Associated Company or Network Member).

5. Maintain complete and accurate records (either in electronic format, hard copy format, or both, provided their indexing, storage, preservation, and reproduction are accurate and complete) of the documentation obtained during the application validation stage as proof of application integrity and time of processing. These records for the avoidance of doubt must include all relevant information in a Unipass Controller's possession regarding:
    a. evidence of identity of each applicant as a bona fide member of an Organisation, Associated Company or Network Member;
    b. the compliance of each Certificate applicant with their obligations;
    c. evidence that (a.) and (b.) above were positively checked for each such member immediately prior to submitting any application for a Certificate on that Individual's behalf to OSIS. The date and time of the check must be positively recorded.

6. Retain any records passed to you or maintained by any previous Unipass Controller within your Organisation and/or (if applicable) any Associated Company or Network Member.

7. Immediately notify the Unipass Helpdesk if you cease to act as a Unipass Controller (by sending an email to customerservices@origo.com or by calling 0131 385 8888) and advise them of the identity of any replacement Unipass Controller and the date from which the replacement is to take effect.

8. Ensure that when you cease to act as a Unipass Controller you pass or make available to either your Organisation or any replacement Unipass Controller the records that you have taken in accordance with paragraph 5 above and/or retained in accordance with paragraph 6 above. Whenever possible you should ensure that there is a replacement Unipass Controller in place who also holds an Individual Certificate before you cease to act as a Unipass Controller.

* Please note that an "Associated Company" is a subsidiary of your Organisation, a holding company of your Organisation or a subsidiary of such a holding company (effectively a sister company of your Organisation). Please also note that a Unipass Controller is only allowed to process applications for "Associated Companies" where that Unipass Controller belongs to an Organisation which is a provider of financial products within the UK financial services industry (which OSIS refer to as "Product Provider Organisations").

Please note that a "Network Member" is a member of a "Network Organisation", which in turn is an organisation that has official members conducting business within the UK financial services industry and which takes responsibility for the actions and omissions of its members (e.g. a directly authorised independent financial services intermediary which has appointed representatives). Please also note that a Unipass Controller is only allowed to process applications for "Network Members" where that Unipass Controller belongs to a Network Organisation.

Nominated Person Requirements (in respect of the obligation on Organisations to ensure that employees, partners, principals, directors, officers or sub-contractors ("Staff") who wish to act as "Nominated Persons" comply with these requirements)

1. The member of Staff must be a responsible and experienced individual within your Organisation or engaged by your Organisation who is capable of acting with due care and skill.

2. The member of Staff must be a trustworthy and competent individual who is capable of (i) keeping accurate records of all applications by his or her Organisation and/or any Associated Company or any Network Member (if applicable) for Organisation Certificates, (ii) verifying and validating the details within Organisation Certificate applications and (iii) notifying OSIS promptly when he or she receives a request from the Organisation or any Associated Company or Network Member that its Organisation Certificate be revoked.

The member of Staff has never been the subject of a disciplinary action or proceedings during the course of his or her employment or other engagement with your Organisation.

The member of Staff has not been convicted of any crimes (except minor traffic offences) and is not subject to any criminal charges or investigations.

Nominated Person Guidelines (to be followed by Nominated Persons)

1. Obtain authority from your Organisation's contract signatory to represent your Organisation and/or "Associated Company" or "Network Member" * (if applicable) in the role of Nominated Person.

2. Applications for Organisation Certificates shall be made by Nominated Persons only. Nominated Persons shall contact OSIS via the OSIS Help Desk by E-mail to customerservices@origo.com.

3. Once contact has been established, OSIS will issue to the Nominated Person an application form to be populated, and a data protection policy consent form to be signed. Both should then be returned to OSIS at the following address:

   Unipass Administration
   7 Lochside View
   Edinburgh Park
   Edinburgh
   EH12 9DH.

3. Upon receipt of all required documentation from the Nominated Person, OSIS will complete data validation in accordance with Section 5 of the OSIS Certification Practice Statement ("CPS").

4. Promptly request the revocation of an Organisation Certificate for the Organisation or any of its Associated Companies or Network Members whenever:
   a. any of the information within the relevant Organisation Certificate contains, is known or is suspected to be inaccurate or could reasonably be believed to have been compromised;

b. there has been a loss, theft, modification, disclosure or other compromise of the Private Key of the Organisation Certificate;
c. any activation data, such as a password or PIN, used to protect the Private Key of the Organisation Certificate is compromised or suspected to have been compromised;
d. there is a change in the identity of your Organisation, Associated Company or Network Member (e.g. through merger or acquisition, or change of name).

7. Maintain complete and accurate records (either in electronic format, hard copy format, or both, provided their indexing, storage, preservation, and reproduction are accurate and complete) of the documentation processed by you as part of the application stage and of all correspondence relating to your duties as a Nominated Person. Without prejudice to the foregoing, these records for the avoidance of doubt include all relevant information in a Nominated Person's possession regarding:

    a. evidence of the control mechanisms employed to ensure the ongoing security and confidentiality of the Private Key associated with an Organisation Certificate; and
    b. logs relating to the use of the Private Key associated with an Organisation Certificate.

8. Retain any records passed to you or maintained by any previous Nominated Person for your Organisation and (if applicable) for any Associated Company or Network Member.

9. Immediately notify OSIS if you cease to act as a Nominated Person (by sending an email to customerservices@origo.com) and advise OSIS of the identity of any replacement Nominated Person and the date from which the replacement is to take effect.

10. Ensure that when you cease to act as a Nominated Person you pass or make available to either your Organisation or any replacement Nominated Person the records that you have taken in accordance with the above guidelines. Whenever possible you should ensure that there is a replacement Nominated Person in place before you cease to act as a Nominated Person.

* Please note that an “Associated Company” is a subsidiary of your Organisation, a holding company of your Organisation or a subsidiary of such a holding company (effectively a sister company of your Organisation). Please also note that a Nominated Person is only allowed to process applications for “Associated Companies” where that Nominated Person is engaged by an Organisation which is a provider of financial products within the UK financial services industry (which OSIS refer to as “Product Provider Organisations”).

Please note that a “Network Member” is a member of a “Network Organisation”, which in turn is an organisation that has official members conducting business within the UK financial services industry and which takes responsibility for the actions and omissions of its members (e.g. a directly authorised independent financial services intermediary which has appointed representatives). Please also note that a Nominated Person is only allowed to process applications for “Network Members” where that Nominated Person belongs to a Network Organisation.