

EISS Self Assessment - Section 1 - Information Management Standards

| EISS Specific Section Reference: | | Objective or Procedures | (Responsible Functional Area) | | | | | | Compliant (Y/N) | Action Plan if Needed: | Target Date: |
|---|--|---|--|------|-------|-------|-----------|-------|-----------------|------------------------|--------------|
| | | | Risk | User | Owner | Admin | Custodian | Other | | | |
| 1.0 Information Management Standards | | 1.1.1 Ownership of Information | | | | | | | | | |
| 1.1.a | | Does all data on SDLC computers or networks exist for the purpose of conducting SDLC business? | Integrity | x | x | x | | | | | |
| | | 1.1.2 Access to Information | | | | | | | | | |
| 1.1.2.a | | Is access to the information provided on a "need to know" basis? | Confidentiality | | x | | | | | | |
| | | 1.1.3 Appropriate Usage | | | | | | | | | |
| 1.1.3 | | Is there evidence of usage of any SDLC electronic device for private or personal purposes without direct management knowledge and tacit approval? | Integrity | | | x | | | | | |
| | | 1.2.1 Custodians Role and Authority | | | | | | | | | |
| 1.2.1.a | | Do custodians of information provide physical and procedural safeguards as needed per the classification of information in their custody to ensure the integrity and confidentiality of information assets as identified by information asset owners? | confidentiality integrity | | x | | x | | | | |
| 1.2.1.b | | For each information system, is an owner and delegate clearly defined and documented? | availability | | x | | | | | | |
| 1.2.1.b | | Does the custodian have a list of system owners (SIC 8.1.2)? | Integrity | | x | | | | | | |
| 1.2.1.c | | Does the custodian inform information asset owners of their responsibilities associated with the ownership and security of their data? | Integrity | | x | | | | | | |
| 1.2.1.d | | Do custodians understand that they must not reclassify information without the permission of the owner? | Integrity | | x | | | | | | |
| | | 1.2.2 Owners Role and Authority | | | | | | | | | |
| 1.2.2.a | | Are all information assets accounted for? | Integrity | | x | | | | | | |
| 1.2.2.a | | Do all information assets have a defined owner? | confidentiality integrity | | x | | | | | | |
| 1.2.2.b | | Have owners performed a risk analysis to determine, identify, and document the security classification associated with the information assets they own in accordance with POPI classifications? | confidentiality availability integrity | | x | | | | | | |

EISS Self Assessment - Section 1 - Information Management Standards

| EISS Specific Section Reference: | Objective or Procedures | Risk | (Responsible Functional Area) | | | | | | Compliant (Y/N) | Action Plan if Needed: | Target Date: |
|----------------------------------|---|--|-------------------------------|-------|-------|-----------|-------|--|-----------------|------------------------|--------------|
| | | | User | Owner | Admin | Custodian | Other | | | | |
| | | | | | | | | | | | |
| 1.2.2.b | Is this classification reviewed at a minimum annually? | confidentiality | | x | | | | | | | |
| 1.2.2.c | Do owners ensure that the appropriate business controls are applied and the conditions surrounding the custody or use of their information is in accordance with the requirements of SIC Section 8 and the SDLC EISS? | confidentiality integrity availability | | x | | | | | | | |
| 1.2.2.d | Do owners assign the role of custodian to their data? | confidentiality integrity availability | | x | | | | | | | |
| 1.2.2.e | Do owners fully understand any custodian conditions surrounding the custody or use of their information? | confidentiality | | x | | x | | | | | |
| 1.2.2.e | Do owners ensure the custoditions are in accordance with the requirements of SIC Section 8 and the SDLC EISS? | | | x | | x | | | | | |
| 1.2.2.f | Do owners grant access privileges to those needing access to their data on a need to know basis? | confidentiality | | x | | | | | | | |
| 1.2.2.g | Do owners review access privileges to their data at a minimum annually? | confidentiality | | x | | | | | | | |
| 1.2.2.g | Is this review process documented? | confidentiality | | x | | | | | | | |
| 1.2.2.g | Is renewal information retained for a minimum period of one year? | Integrity | | x | | | | | | | |
| | 1.3 Information Classification | | | | | | | | | | |
| 1.3 | Do information owners define information classification? | confidentiality integrity | | x | | | | | | | |
| | 1.3.5 Assigning Classifications | | | | | | | | | | |
| 1.3.5.a | Has the organization that "owns" the information (usually the creator) determined its sensitivity and criticality classification? | integrity confidentiality | | x | | | | | | | |
| 1.3.5.b | Has the information been classified according to Corporate SOP E-60? | confidentiality | | x | | x | | | | | |
| 1.3.5.c | Has proprietary information and information that is highly sensitive to outages been identified in disaster recovery plans as described in Section 8 of SDLC's EISS? | availability | | x | | x | | | | | |

EISS Self Assessment - Section 1 - Information Management Standards

| EISS Specific Section | | | | | | | | | |
|-----------------------|--|-------------------------------|-----------------|-------|-------|-----------|-------|------------------------|--------------|
| Reference: | Objective or Procedures | (Responsible Functional Area) | Compliant (Y/N) | | | | | Action Plan if Needed: | Target Date: |
| | | Risk | User | Owner | Admin | Custodian | Other | | |
| 1.3.5.d | Have the information classifications been reviewed at a minimum annually by the business unit that owns the information to ensure that the classification is still correct? | confidentiality | | x | | | | | |
| | Classifications of Data Output | | | | | | | | |
| 1.3.5.e | Is output, including report, data, and software, which contains the same information content as the input used to create it assigned the same sensitivity classification as the input? | confidentiality | | x | | | | | |
| 1.3.5.f | Is output that is formed by the merger of multiple inputs classified in accordance with the highest level of sensitivity classification represented by the input? | confidentiality | | x | | | | | |
| 1.3.5.g | Is output that is substantially different than the input information used to create it, classified independently from the input? | confidentiality | | x | | | | | |
| | Access | | | | | | | | |
| 1.3.5.h | Do system or application "owners" authorize access to their data or applications in accordance with SIC 8.3.5? | confidentiality | | x | | | | | |
| 1.3.5.i | Is access authorization reviewed on a yearly basis in accordance with SIC 8.3.5? | confidentiality | | x | | | | | |
| | 1.3.7 Non-SDLC Proprietary Classification | | | | | | | | |
| 1.3.7.a | Does the SDLC representative ask a non-SDLC information owner to define the meaning of any non-SDLC information classification label? | confidentiality | | | | x | | x | |
| 1.3.7.b | Is the non-SDLC proprietary classification, along with the SDLC equivalent classification marked on information which is not owned by SDLC and is it considered proprietary based on the original owner's classification scheme? | confidentiality | | | | x | | | |

EISS Self Assessment - Section 1 - Information Management Standards

| EISS Specific Section | | Compliant (Y/N) | | | | | | Action Plan if Needed: | | Target Date: |
|--|---|-------------------------------|------|-------|-------|-----------|-------|------------------------|--|--------------|
| Reference: | Objective or Procedures | (Responsible Functional Area) | | | | | | | | |
| | | Risk | User | Owner | Admin | Custodian | Other | | | |
| 1.3.7.c | Is the use of non-SDLC proprietary information while in the possession of SDLC treated with the same care as defined by the closest corresponding SDLC POPI classification? | confidentiality | | | | x | | | | |
| 1.4 Information Privacy Standards | | | | | | | | | | |
| 1.4.a | Are regional and local in Country Management, with guidance and advice from local Corporate Legal departments responsible for ensuring compliance with in Country and regional legislation? | confidentiality | | | | | Mgmt | | | |
| 1.4.b | Do regional and local in Country Management ensure that SDLC Ethics principles are enforced and that the individual's personal and business privacy is not willfully violated? | confidentiality | | | | | Mgmt | | | |
| 1.4.c | Are management and especially Human Resources diligent when handling employee Personal and private data? | confidentiality | | | | | Mgmt | | | |
| 1.4.c | Does the information system handling personal and private data comply with applicable data protection laws, which may also cover manual records? | confidentiality | | | | | Mgmt | | | |
| 1.4.d | Is accidental disclosure of personal data, for example in the course of problem resolution, kept to an absolute minimum? | confidentiality | | | | | Mgmt | | | |
| 1.4.e | Does information system handling of personal and private data comply with applicable protection laws? | | | | | | Mgmt | | | |
| 1.4.f | Is a person assigned at each SDLC unit to take responsibility for ensuring compliance with these privacy standards, and national and international legal requirements, including registration with Data Protection Authorities? | confidentiality | | | | | Mgmt | | | |