## Terms and Definitions

Table below summarizes the terms as used within this SCG and associated definitions.

| Term | Definition |
|---|---|
| Administrator/ Privileged User | Person who manages user privileges and accounts of the **EPS**. This person can be a GC resource or **EPS** contractor resource. |
| Classification Level | An indicator or the sensitivity of the **EPS** information, i.e.: Protected A, Protected B, Unclassified, and other classifications specified by Government of Canada (GC). |
| Client | Any GC-owned or managed user agent or application that connects to the **EPS**. |
| Contractor | The person, entity or entities named in the Contract to supply goods, services or both to Canada |
| **EPS** Data | All data associated with **EPS**, including EPS User Data, **EPS** Operational Data, on any media. |
| **EPS** Operational Data | Any administration and management data generated by the **EPS** Infrastructure, on any media, such as security violations, transactions, audit records, alarm incident records, reports, logs, backups. |
| **EPS** Infrastructure | All hardware and software that processes and stores EPS Data and that Operators use to manage **EPS**. |
| External End Users | A Non-GC person that is authorized to use the **EPS**. |
| GC End Users | A GC resource (employee, contractor, etc.) that is authorized to use the **EPS**. |
| Host | Means any Internet Protocol (IP) addressable entity connected to an IP-based network. |
| Incident | Event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. |
| Incident Management | Standardized methods and procedures to restore a service to normal operation as quickly as possible and to minimize the impact on business operations |
| Contractor Operations Centre | Contractor location that includes infrastructure and resources required for the centralized management and operation of the **EPS**. There are Two types of operations centers<br>a. Network Operations Center (NOC), and<br>b. Security Operations Center (SOC). |
| Operator | A Contractor resource which administers **EPS** Infrastructure. |
| Problem | Unknown cause of one or more Incidents, often identified as a result of multiple similar Incidents |
| Problem Management | Standardized methods and procedures to minimize the impact of Problems for **EPS**. |
| Public User | General population or community that is not an authorized user of the **EPS**. |
| Public/Open Data | Information that has no classification as it covers or details publicly available information. |
| Material Resource | A Room or Equipment. |
| Secure Perimeter | Logical and physical boundary around network accessible resources and information, which is controlled and protected against unauthorized access from outside of the boundary. |

| Term | Definition |
|---|---|
| Security Incident | An unauthorized behaviour (against the security policy of the IT system) regarding the operation and administration of the IT system that has the potential to compromise the IT systems confidentiality, integrity, or availability. |
| Managed Service | An electronic service configured, implemented, operated and managed by the service provider, including the supporting software, infrastructure, upgrades, maintenance and support. |
| Service Delivery Point (SDP) | Physical location in a building where the **EPS** is implemented. |
| Solution User Data | Includes Account, Notifications, Customized views and filters. |
| Supplier | Represents External users of the **EPS** that will be using the **EPS** to offer their services in response to various tenders published by GC. |

Table below outlines the personnel and facility security clearance requirements based on the expected roles, high-level EPS data access, and location of the data access.

| # | Role/Function | Expected Type of Data Accessed | Data Access Location (Canada/Foreign /Both) | Expected Data Sensitivity Classification Level | Clearance Level |
|---|---|---|---|---|---|
| 1. | Public Users who will need to access 'Open/Public' information related to tenders being posted or contracts awarded by GC through the EPS. | • Public/Open Business Data;<br>• Contract Award Notifications (CANs) in the EPS;<br>• Very Limited Financial Information (Only the actual value of the Contract as identified in the CAN in the EPS). | Both (refer to information flow IF-A in Figure 1 below) | N/A | N/A |
| 2. | External End Users including the supplier delegates who will need to access the information specific to their business and bid responses including company proprietary information. | • Business Data;<br>• User credentials (each supplier has ownership of the assigned unique users accounts);<br>• RFP submissions and associated supplier propriety information;<br>• Supplier's financial information | Both (refer to information flow IF-A, IF-D, IF-E in Figure 1 below) | N/A[1] | N/A |
| 3. | Any EPS Contractor personnel with physical access to the EPS infrastructure at Contract Service Delivery Points (SDP), includes Contractor data centers, Security Operations Center (SOC), Network Operations Center (NOC).<br><br>Additionally, physical segregation requirements will | • Physical hardware;<br>• Service Delivery Point (Data Center Contractor / SSC);<br>• Data as stored on the Contractor's local Backup Media | Canada (refer to information flow IF-C in Figure 1 below) | Protected 'B' | Secret[2] |

[1] Information local to supplier is not sensitive to them. Once it is handed over to GC, it is deemed as Protected 'B'.
[2] This will be mandated by the deployment model assuming it involves SSC Data Center facilities.

| # | Role/Function | Expected Type of Data Accessed | Data Access Location (Canada/Foreign /Both) | Expected Data Sensitivity Classification Level | Clearance Level |
|---|---|---|---|---|---|
| | be separately identified within the EPS Contract. | | | | |
| 4. | Contractor Personnel during High Level Design (HLD) Phase | • Design Blueprint;<br>• COTS products configuration details;<br>• Hardware details;<br>• Security policy and rules as applicable to EPS including perimeter controls and auditing | Both (Information Flow not applicable here) | Protected 'B' | Enhanced Reliability |
| 5. | Contractor Key Resources providing services on the solution development and delivery team for the EPS | • Design Blueprint;<br>• COTS products configuration details;<br>• Hardware details;<br>• Security policy and rules as applicable to EPS including perimeter controls and auditing | Both (Information Flow not applicable) | Protected 'B'[2] | Enhanced Reliability |
| 6. | Contractor Application Integration Support as required through the design and development phases of the EPS | • Design Blueprint;<br>• COTS products configuration details;<br>• Hardware details;<br>• Security policy and rules as applicable to EPS including perimeter controls and auditing | Both (Information Flow not applicable here) | Protected 'B'[2] | Enhanced Reliability |
| 7. | Contractor Security Operations Center(SOC) Personnel | • All Business Data;<br>• Security Data including audit logs;<br>• System configuration including security components;<br>• Physical hardware;<br>• Service Delivery Point | Canada (refer to information flow IF-C in Figure 1 below) | Protected 'B'[2] | Secret |

| # | Role/Function | Expected Type of Data Accessed | Data Access Location (Canada/Foreign /Both) | Expected Data Sensitivity Classification Level | Clearance Level |
|---|---|---|---|---|---|
| | | (Data Center Contractor / SSC);<br>• Backup Media | | | |
| 8. | Contractor Operations Center Personnel | • All Business Data;<br>• Security Data including audit logs;<br>• System configuration including security components;<br>• Physical hardware;<br>• Service Delivery Point (Data Center Contractor / SSC);<br>• Backup Media | Canada (refer to information flow IF-C in Figure 1 below) | Protected 'B'[2] | Secret |
| 9. | Contractor Service Desk Personnel | • All Business Data including RFP response for incident trouble shooting;<br>• Security Data including login credential;<br>• System configuration including security components;<br>• Reporting;<br>• Service Delivery Point (Data Center Contractor);<br>• Incident ticketing system | Both (refer to information flow IF-C in Figure 1 below) | Protected 'B' | Enhanced Reliability |
| 10. | Contractor's 4th Level Original Equipment Manufacturer (OEM) Support Personnel | • Business Data;<br>• Security Data including login credential;<br>• System configuration including security components;<br>• Service Delivery Point (Data Center | Both (refer to information flow IF-C in Figure 1 below) | Protected 'B' | N/A |

| # | Role/Function | Expected Type of Data Accessed | Data Access Location (Canada/Foreign /Both) | Expected Data Sensitivity Classification Level | Clearance Level |
|---|---|---|---|---|---|
| | | Contractor);<br>• Incident ticketing system | | | |

# EPS Human Interface – Information Flows

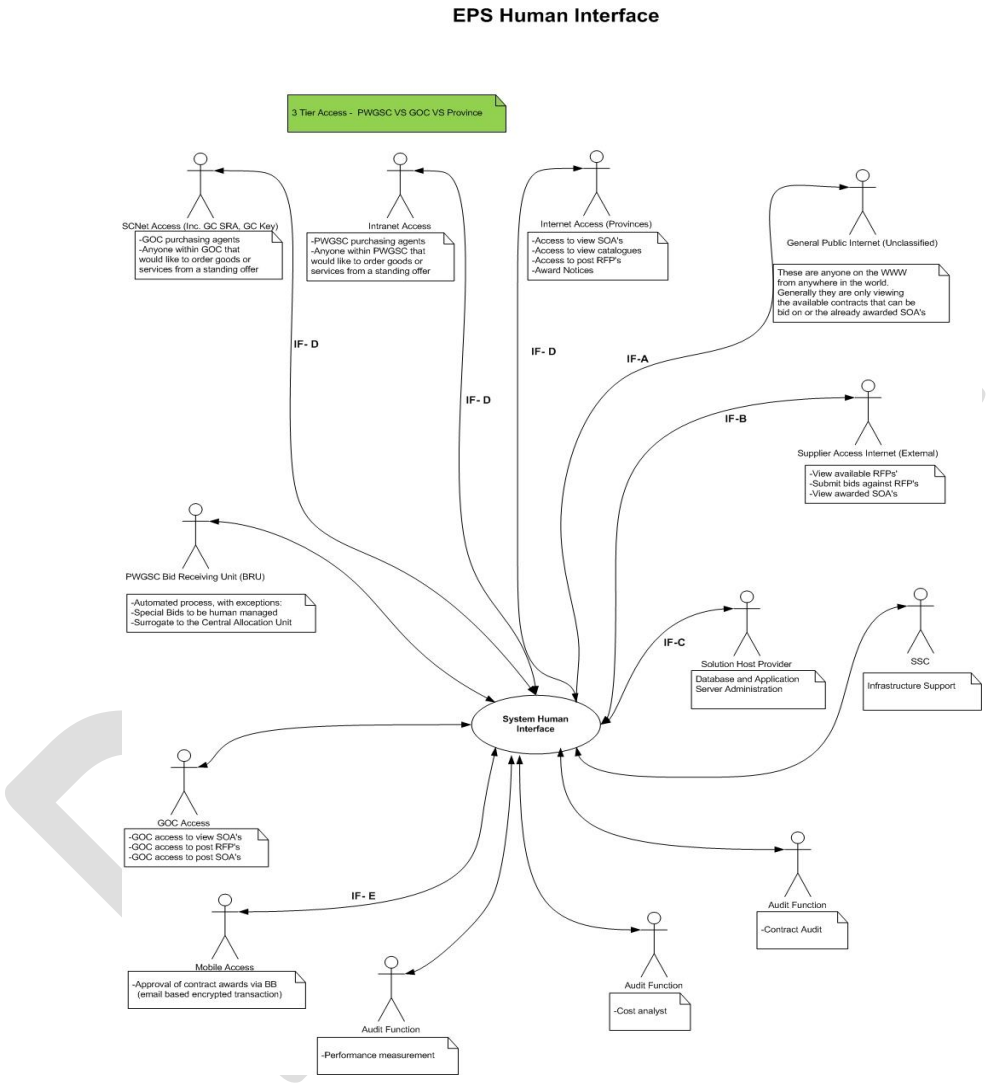


**Figure 1: EPS - Human Interfaces Information Flows**