LIABILITY

FPDI states that it has no relationship with, and owes no duty whatsoever to anyone who is not the SAH as detailed in the Agreement. FPDI will not be liable and expressly disclaims all liability whatsoever to anyone or to any entity who is not a Service Provider or Third Party as defined in the Agreement for any claims, actions, loss, damages, awards, including without limitation, loss of revenue or profit or savings, lost or damaged data, or other commercial or economic loss, or any indirect or incidental, special or consequential damages, whatsoever, even if FPDI has been advised of the possibility of such damages, or for claims by an individual, organization or entity not Party to the Agreement, nor shall FPDI's contractors, suppliers, agents, employees or representatives have such liability.

The SAH agrees to take full responsibility for all actions of the Authorized Users, including those who are employees, agents and contractors of Service Providers acting within the scope of the duties and functions of their employment or contract.

INTRODUCTION

What is a Service Level Agreement (SLA)?

A Service Level Agreement (SLA) is an official commitment that is between a Service Provider (FPDI) and a Client (Recipient/ Sub-Agreement Holder or SAH).

What is it used for?

The SLA is used for the protection of personal information and systems and security requirements for exchanging information and data under the Aboriginal Skills and Employment Training Strategy Funding Agreement (ASETS).

FPDI and the Recipient (SAH) are committed to ensuring that the Personal Information they provide to each other under the ASETS Funding Agreement is reliable and provided in a timely, secure and confidential manner and FPDI and the SAH have agreed to work together to achieve this goal.

The SAH is responsible for:

- Ensuring that all Personal Information (e.g. client information) in the care and control of the SAH or a Third Party (Service Provider) is protected from misuse and unauthorized access, disclosure, modification, disposal or destruction at all times;
- Ensuring that the identification and authorization information of a SAH or SAH staff or Authorized User collected in support of the application for accessing Systems and Services Administered by Canada is accurate and complete, and that the FPDI Administrative Assistant Theressa West is immediately advised if any of that information changes or is no longer valid or accurate;
- Managing, supporting and maintaining its own technological environment including its network, routers and workstations.

ACCESS and SHARING

Personal information can only be accessed and shared on a “need-to-know” basis.

To be granted access to the Systems and Services Administered by Canada listed in the Service Level Agreement, all SAH staff must undergo a personnel security screening process and obtain a valid Reliability Status as per the SSOG (Systems Support Operational Guide). FPDI will perform the required security screening process for the SAH or staff who require access.

FPDI will provide the SAH and staff or any Third Party identified by the SAH with access to information for systems and services for the purpose of exchanging Personal Information in accordance with the ASETS Funding Agreement. FPDI also has discretion to refuse a personnel security screening of any staff provided by the SAH.

The SAH and staff will monitor system usage to ensure Authorized User compliance with the terms of the Agreement and will immediately advice FPDI with details of any misuse and unauthorized access, disclosure, modification, disposal or destruction in the event that any misuse is suspected or identified through the processes and procedures described in the SSOG.

PUBLIC AREAS

All SAH’s publicly accessible areas must be kept clear of Personal Information except when client’s files are under the direct care and control of a SAH or staff.

NIGHTLY CLOSING

All SAH’s, staff and Third Parties must remove all Personal Information from their desks and store it in locked filing cabinets before they leave for the day.

They also must remove all documents containing Personal Information from printers and fax machines and place the documents in a locked cabinet. All SAH’s and staff must also log out of all computers and lock the doors and secure the premises (e.g. enabling the alarm system and locking the doors etc.).

MAILING in CANADA

Personal Information in the care and control of the SAH, staff or their Third Parties MUST be transmitted (distributed) as letter-mail in a double envelope (e.g, window-less envelope sealed in larger outer envelope), gum-sealed, with no security markings on the outer envelope.

TRANSPORTATION in CANADA

All paper records with Personal Information in the care and control of the SAH, staff or Third Party that are transported outside of a controlled area must be in a double envelope, gum-sealed, with no security markings on the outer envelope and appropriately addressed.

In instances where delivery is urgent, transportation should be managed by a reliable courier services or similar postal service with a record of transit and delivery, packaged as for communication letter mail.

ELECTRONIC STORAGE and TRANSMISSION

Electronic storage and transmission of files and/or databases containing Personal Information in the care and control of the SAH and staff or Third Parties may only be authorized where:

- Personal Information is password protected at all times while in transit;
- Personal Information is protected at all times while in storage;
- Information technology and Systems involved in managing Personal Information fully comply with policies, procedures and guidelines described in the SLA.

PHYSICAL STORAGE

Storage of physical documents containing Personal Information in the care and control of the SAH, staff or Third Party is permitted:

(a) Temporarily, on open shelving within areas that are continually monitored and where access is controlled and limited to authorized personnel of the organization or security staff; and
(b) Using locked cabinets or secure containers.

E-MAIL

Only the minimum necessary information required to deliver services under the ASETS program should be exchanged via email.

Personal Information should only be transmitted electronically by the SAH and staff or Third Parties by first putting the information in a password protected document and then appending the document to an email. The password for the appended document should then be subsequently shared either by phone or by using a separate email ("password" must NOT be specified in the subject line) with the authorized party receiving the appended document.

To see how to set up Password Protected Documents, turn to page 10.

FAX TRANSMISSION

Personal Information can only be faxed between parties using a secure fax equipped with the appropriate and compatible security software.

PAPER RETENTION and DESTRUCTION

All paper records with Personal Information in the care and control of the SAH, staff or Third Parties MUST be retained for a period of six (6) years after completion of the agreement as per Schedule D, Section 16 (b) of the ASETS Funding Agreement.

Once this six (6) year period is complete, paper records MUST be destroyed using a commercially available strip-cut shredder or a secure recycle bin.