SmartFile Data Breach Response Policy

1. **Purpose**
   SmartFile is committed to protecting customers, employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy establishes the breach response process for SmartFile, including the definition of a breach, staff roles and responsibilities, reporting, remediation, and feedback mechanisms.

   Any individual who suspects that a theft, breach or exposure of Protected data or Sensitive data has occurred must immediately provide a description of what occurred via e-mail to support@smartfile.com or through the use of the help desk reporting web page at https://support.smartfile.com/. Our team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred, and if it has, will follow the appropriate procedure in place.

2. **Scope**
   This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Protected data or Sensitive Data.

   “Protected Data” are customer-owned data that are stored on SmartFile’s file sharing platform.

   “Sensitive Data” are personally identifiable data on SmartFile’s customers that are used for providing service.

3. **Confirmed theft, data breach or exposure of Protected data or Sensitive data**
   As soon as a theft, data breach or exposure containing Protected data or Sensitive data is identified (a “confirmed incident”), the process of removing all access to that resource will begin. The Chief Technology Officer will chair an incident response team to handle the breach or exposure. The team will include members from:

   - Engineering operations and development
   - Finance
   - Customer support
   - Legal
   - Communications
   - The affected customer or customers whose data may have been breached or exposed

      a. **Incident Response**

The designated team will immediately take all steps necessary to prevent further compromise of Data, and then will analyze the breach or exposure to determine the root cause.

As provided by SmartFile cyber insurance, we may need to provide access to forensic investigators and experts to determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

b. **Communication plan**

The designated team will work with communications, legal and human resource departments to determine how to communicate the breach to entities directly affected and to the public.

Once it has been determined that an entity is affected by a confirmed incident, the affected party will be notified within 24 hours, and will be provided with a written report within three days thereafter. SmartFile will respond to all reasonable requests by the affected party for information pertaining to the confirmed incident.

c. **Remediation**
The designated team will work promptly to repair or remediate the vulnerabilities which were exploited in the incident. This may include, for instance, software changes, business processes changes, changing vendors, or personnel actions. In addition, efforts will be taken to mitigate the risk of further incidents.

d. **Reporting**
Upon conclusion of investigative, corrective, and remedial actions with respect to the confirmed incident, a final report will be created and shared with affected entities that describes the incident, the affected data, supporting evidence, and corrective and remedial actions taken.

4. **Definitions**

- Protected Data – Data owned by a customer of SmartFile, that is stored on SmartFile's infrastructure

- Sensitive Data –PII data belonging to a customer that is used by SmartFile in the provision of service to that customer. This includes, for example, payment information,

phone numbers, and address information.

- Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual.

5. **Revision History**

Version	Date	Author	Description of Changes
1.0	April 25, 2018	Tony Spelde	Initial version