Data Breach Notification Policy

This policy sets out how Solenis manages Security Incidents and Personal Data Breaches. Solenis is committed to handling Personal Data securely and properly. Lawful handling of Personal Data consistent with this policy is vital to our successful business operations. The purpose of this policy is to provide clear guidelines on how to identify and deal with a Security Incident, which may constitute a Personal Data Breach. This policy applies to all Solenis employees (which includes temporary and permanent employees, contractors, consultants and others) and any other individual whose personal data we process in the course of doing business, including customers, vendors, job candidates and other business partners.

This policy is not intended to override any local laws that may impose specific duties on how to respond to a Security Incident; instead, it acts as an overarching framework to help us identify and manage Security Incidents in a consistent manner across our business. Where you are aware of conflicting or additional local legal or regulatory requirements, you should comply with those requirements as a matter of routine, but where feasible do so in a manner consistent with this policy.

Any defined terms used within this policy are set out in Appendix 1 (Definitions).

2.0 Responsibilities

It is the responsibility of all employees to assist Solenis in complying with this policy. The table below provides a summary of responsibilities for the key roles referred to throughout this policy:

ROLE	RESPONSIBILITY
Office of Data Privacy	• Oversee overall compliance throughout Solenis and ensures that each party meets its responsibilities.
Information Security Global Information Technology team	• Advise as to whether Security Incidents are in fact Personal Data Breaches. • Ultimate responsibility for managing suspected Personal Data Breaches with support from other business functions as needed, including preparing incident management plans. • Triage with the Security Incident to the extent necessary.
Legal	• Advise as to whether a Security Incident constitutes a Personal Data Breach. • Provide legal assistance and if necessary, work with an outside legal counsel. • Advise on legal ramifications of the breach. • Confirm regulatory requirements and assist in creating official notifications. • Notify relevant supervisory authorities.
Affected business unit management	• Provide business unit perspective and buy-in for response actions. • Support business unit manager with the incident management plan.

All employees	• Take steps to prevent Personal Data Breaches and report Personal Data Breaches appropriately.

3.0 Detecting and responding to a Personal Data Breach

We have a four-step approach to dealing with Security Incidents or potential Personal Data Breaches involving (1) detection, (2) assessment, (3) response handling and (4) reporting and review. Each step will be tailored to the specific circumstances of each Security Incident or potential Personal Data Breach. Each of these steps are explained in more detail below.

3.1 Step 1 – Detection

We expect Security Incident or potential Personal Data Breaches to be detected through the following channels:

- **Employee reporting –** Employees are expected to be mindful of any Security Incident or potential Personal Data Breaches and immediately report to the Information Security Global Information Technology team concerns that have or may have arisen in or, when relevant, to the Office of Data Privacy.
- **Monitoring by Information Security –** We routinely monitor our IT systems to detect Security Incidents and potential Personal Data Breaches. Most minor Security Incidences where there is no risk of a Personal Data Breach will be dealt with directly by our Information Security Global Information Technology team (e.g., minor breaches of acceptable use policies, etc.). More serious Security Incidents and any possible Personal Data Breaches are expected to be escalated to the Office of Data Privacy.
- **External notifications –** Employees are expected to be proactive in escalating any information provided by third parties about any Security Incident or potential Personal Data Breaches to the Information Security Global Information Technology team or, when relevant, to the Office of Data Privacy. Employees should treat all reports of Personal Data Breaches occurring at third party processors as (for all practical purposes) reports of breaches of Solenis systems, to be escalated accordingly.

3.2 Step 2 – Assessment

When a Security Incident or Personal Data Breach is detected and notified in accordance with the above, an initial assessment will be undertaken, and triage process commenced. This will involve: (i) advising on any immediate steps to be taken (e.g., changing user passwords); (ii) further internal escalation and involvement of relevant stakeholders (if required), and (iii) recording the Security Incident or potential Personal Data Breach. Where necessary and appropriate, the Office of Data Privacy is to provide more detailed assessment on the nature and scope of any Security Incident or Personal Data Breach escalated to it. If necessary, the Office of Data Privacy will establish a response team, which will be led by an incident manager.

3.3 Step 3 –Reporting and Notification

The action to be taken in response to the Personal Data Breach will be decided by Information Security Global Information Technology Team, the Office of Data Privacy or the response team (if established). The action to be taken will depend on the nature of the Personal Data Breach. This may include: **investigation:** to

understand the nature of the incident, the impact on Solenis, help establish the underlying cause and establish impacted internal and external stakeholders; **containment and mitigation of the breach:** to prevent any further data loss or security compromises, which may involve taking systems offline; **restoration:** of any services impacted by the breach as soon as possible once the breach has been contained; **engagement with stakeholders:** which is likely to include employees, the media, customers and appropriate regulators or law enforcement agencies. An engagement plan should be agreed upon by the Legal and Corporate Communications departments at the earliest opportunity, and **reporting:** to regulators, affected natural persons, and other organizations or government institutions that Solenis believes can reduce or mitigate the risk of harm that could result from the breach to the extent required by applicable laws.

Guidance from the Office of Data Privacy must always be sought before engaging employees or any external stakeholders to ensure information disclosed is accurate and does not expose Solenis to undue risk.

Guidance from Solenis' Legal department must be always sought to determine whether and how to report Security Incident or Personal Data Breaches to affected individuals, customers or regulators.

The Corporate Communications department must be involved in handling interactions with the media and to develop a timely communication strategy, including preparation of a proactive statement to be released.

3.4 Step 4 - Incident reporting and review

- If appointed, the incident manager will coordinate the notification of all parties that the incident is resolved. Otherwise, the Information Security Global Information Technology team or the Office of Data Privacy will decide what further communications may be required regarding this (if any).
- The Information Security Global Information Technology Team, the Office of Data Privacy or the incident manager (as appropriate) will produce an Incident Report and will perform the post-incident review.
- The Incident Report will include in particular (without limitations): summary of the incident; actions taken with dates and action owners; an estimate of the financial cost and business impact of the incident; recommendations for changes to avoid future occurrences and any lessons that could be learned from the incident.
- The Information Security Global Information Technology Team, the Office of Data Privacy or the incident manager (as appropriate) will hold a post-incident review meeting with all parties involved.

4.0 Response team

If established, the exact membership of the response team will depend on the nature of the Security Incident or Personal Data Breach, but is likely to include representation from each of the following key business functions, with the respective responsibilities as listed: Regional Legal Counsel, Information Security Officer, Corporate Communications and Human Resources. In addition, the response team will be led by the incident manager, who will be the point of responsibility for the resolution of the Security Incident or Personal Data Breach and the production of the Incident Report.

This policy requires the response team to log all Personal Data Breaches or potential Personal Data Breaches discovered during the investigation according to guidelines provided by the Office of Data Privacy and to submit the report to Office of Data Privacy.

Appendix 1: Definitions

In order to fully appreciate the requirements of applicable data privacy legislation it is important for you to understand the meaning of certain key words and phrases used within this policy.

"Data Processor" shall mean the person or company who processes Personal Data on behalf of the Data Controller.

"Data Controller" shall mean the person or company who, either alone or jointly with others, determines the purpose for which, and the manner in which, Personal Data is processed.

"Office of Data Privacy" shall mean selected Solenis employees who (i) supervise, advise and are in charge of all activities related to compliant collection and processing of Personal Data at Solenis; (ii) shall ensure that this policy and all other related policies are properly applied across Solenis; and (iii) are responsible for the oversight and implementation of this policy (including all other related policies); for communicating the policy requirements (including all other related policies), and any revisions made to this policy (including all other related policies). The Office of Data Privacy can be contacted at privacy@solenis.com. For further information regarding the Office of Data Privacy, please visit Solenis InSite at the links provided in this document.

"Data Subject" shall mean an identified or identifiable natural person whose Personal Data is being processed.

"Natural person" refers to an individual human being that is not a legal person (e.g., corporation).

"Personal Data" shall mean any information capable of identifying a natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their his or her physical, physiological, mental, economic, cultural or social identity. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link.

"Personal Data Breach" shall mean a Security Incident resulting and leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

"Processing" or "processing" shall mean any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, including, but not limited to collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction (and Process / process, Processes / processes and Processed / processed shall be interpreted accordingly).

"Security Incident" shall mean a security event that compromises the integrity, confidentiality, or availability of Personal Data.

"Sensitive Personal Data" or **"Special Categories"** of Personal Data shall mean the Special Categories of Personal Data that are considered to be "sensitive," requiring additional care when handling, including health, racial or ethnic origin, sexual life or orientation, religious or philosophical opinions, political opinions, trade union membership, or genetic or biometric data (for the purpose of uniquely identifying a living individual. Also

considered within the Special Categories of Personal Data are criminal history / criminal convictions and data of children 13 years of age and under) and personal bank, credit card or other financial information.

"**Solenis InSite**" shall mean the Solenis intranet, accessible only to Solenis employees and selected contractors, that facilitates an important point of internal communication and is accessible at https://solenis.sharepoint.com/.