This Supply Risk Solutions (SRS) Privacy and Security Policy describes SRS' practices regarding the collection, protection, use and disclosure of the information we collect from SRS customers and their suppliers using SRS applications in any media: web, mobile, email, text, etc. (the “Service”). It is enforced by the SRS CEO who is responsible for compliance. This policy is reviewed at least annually.

Multi-Level Data Security

SRS is committed to data security and has therefore implemented multi-level physical, procedural and technical safeguards in connection with the storage, processing and transfer of data. These safeguards include the following:

- **Hosting in secure Azure data centers** which have achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports;
- **Encryption** of data in transit and at rest;
- **Permission-based access** where organizations control their data in a strictly permission-based website where they can update or delete data at any time and where they determine which other organizations see the data;
- **Data and software resilience** with hourly backups between redundant Azure data centers separated by 2500 miles (4000 km);
- **Physical data center security** including 24x365 guards and monitored operations center;
- **Secure solution architecture** including network security, firewalls, hardened servers, hardened software applications and by making all servers inaccessible from the internet;
- **Monitoring** including log analysis, copying log events to separate server, malware detection, real-time event alerting and active response;
- **Procedural controls** such as security training, minimizing access to production data to few personnel, enabling access only through encrypted, internal VPN;
- **Testing** to prevent unauthorized access, accidental loss, destruction or damage and to ensure timely recovery in the event of an outage.

SRS provides superior data security, control and privacy to all organizations that use SRS software, regardless whether they are customers of SRS, suppliers, or other organizations.

Privacy Protections and Certifications

SRS is committed to maintaining unsurpassed data privacy and data protection compliant with international standards including the EU-US Privacy Shield Framework, the Swiss-US
Privacy Shield Framework, the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act of 2018 and the UK Data Protection Act. SRS is also under binding Non-Disclosure Agreements (NDA) with its customers. You may view Supply Risk Solutions’ active Privacy Shield Framework certification [here](https://www.privacyshield.gov).

SRS is a certified business within the **EU-US Privacy Shield Framework**, which complies with EU and US law and privacy regulations, including the EU General Data Protection Regulation (GDPR). The SRS certification for the EU-US and the Swiss-US Privacy Shield Framework is subject to the investigatory and enforcement powers of the **US Federal Trade Commission (FTC)**. This Framework includes formal, written procedures that protect data privacy. SRS certifies that the SRS Privacy and Security Policy and practices, described in this document, is a public commitment that adheres to the EU-US Privacy Shield Principles ([https://www.privacyshield.gov](https://www.privacyshield.gov)), per Supplemental Principle 6 (Self-Certification), under the FTC’s jurisdiction, effective July 25, 2016 forward and the Swiss-US Privacy Shield Framework.

SRS provides the following in full compliance with EU-US Privacy Shield Principles:

1. **Notice**: Inform data subjects via this detailed online privacy policy. Data subjects can opt out of communications and can update and delete their information themselves at any time using the following websites:
   - Supplier contacts can add, update and delete their Personal Data at any time by logging into the secure website [https://supplier.supplyrisk.com](https://supplier.supplyrisk.com)
   - Customer contacts can update and delete their Personal Data at any time by logging into the secure website [https://customer.supplyrisk.com](https://customer.supplyrisk.com)
   - You may also email our support team at bcmsupport@supplyrisk.com with any questions or requests such as opting out of communications.

2. **Choice**: We will not share your information with a third party for a purpose that is materially different from original purpose (supply chain risk reduction) without your consent. Personal Data (name, job title, email and telephone number) resides in secure software applications that we built and in secure SaaS-based third party technical support and communications systems that we use to support and communicate with our customers and their suppliers.

3. **Security**: SRS safeguards data that it collects with multi-level data security, including leading technology, procedural and policy measures, as described above.

4. **Data Integrity**: Personal Data is limited to what is relevant for the purpose of the processing, namely the contact names, job title, email address and telephone number of our customers and their suppliers. SRS takes measures to ensure that Personal Data is accurate, complete and current.
   - Personal Data is processed fairly and in a transparent manner for specified, explicit and legitimate purposes and kept no longer than is necessary for the purposes for which the Personal Data are processed. SRS maintains a Register of Systems that it uses to process Personal Data and reviews that Register at least annually.
5. **Legal Basis of Processing Personal Data**: SRS processes Personal Data of SRS customers and their suppliers because the processing is necessary for specific legitimate business purposes which include some or all of the following:
   - to fulfill legally binding Master Service Agreements with SRS customers to assess, monitor and reduce supply chain risks
   - to improve the effectiveness of SRS services to suppliers, including natural disaster alerts, secure transfer of data to customers, rapid communication with customers during natural disaster events, etc.
   - to personalize our software
   - to enhance information security, such as by confirming that account information is current and safeguards to data and software access are in place
   - to better understand how people interact with our software
   - to provide communications which we believe will be of interest to you

6. **Access**: Data subjects can obtain confirmation of whether SRS processes Personal Data related to them by emailing bcmsupport@supplyrisk.com or by logging into the websites described above in section “1. Notice”.

7. **Accountability to Onward Transfers**: If SRS wishes to transfer Personal Data to a third party acting as an agent, SRS will ensure that the transfer is made on the basis of a contract which provides the level of protection guaranteed by the Privacy Principles.
   - Personal Data (name, job title, email and telephone number) resides in secure software applications that we built and in secure SaaS-based third party technical support and communications systems that we use to support and communicate with our customers and their suppliers.
   - Generally, SRS remains liable for damages from violation of Privacy Shield Principles by the third party. Exceptions include if SRS proves that it is not responsible for the event giving rise to the damage or if SRS is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

8. **Enforcement and Redress**: Ensure compliance with the Privacy Principles and to put in place an effective redress mechanism. Data Subjects have options for addressing data privacy protection issues, including but not limited to:
   - SRS (recommended, free): Please email any Personal Data protection issues, suggestions or questions to SRS’ CEO Patrick Brennan at bcmsupport@supplyrisk.com. SRS will normally reply within 1-3 business days
     - SRS is not required by GDPR Article 27 to designate a representative in the EU because processing is occasional and does not include on a large scale, processing of special categories of data as referred to in Article 9(1), nor in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing. We offer our Software as a Service solution to companies; no goods or services are offered to data subjects (only to companies).
   - Independent Recourse Mechanism: An individual (“Data Subject”) also has the option to seek recourse through an independent organization named JAMS
JAMS will mediate unresolved complaints at no cost to the Data Subject as explained in Supplemental Principle 11 (Dispute Resolution and Enforcement). JAMS is SRS’ designated alternative dispute resolution provider, for Data Subjects who prefer to use an independent recourse mechanism for addressing privacy protection issues. There is also the possibility, for an individual to invoke binding arbitration, under certain conditions (for example, after exhausting all other options).

SRS processes Personal Data and other collected data only as necessary to
- Maintain, provide and improve the Service of monitoring and reducing risks to SRS customer organizations and their supply chains
- Comply with SRS customer agreements/Statements of Work and the Information Collection and Use section of this policy
- Better understand how our Service is being used
- Address a service request from you
- Comply with or avoid the violation of applicable law, regulation or subpoena

In the unlikely event of a breach involving unlawful or harmful unauthorized access of unencrypted personally identifiable information (PII) or other confidential information, SRS policy is to notify and work with affected SRS customers within 24 hours and authorities within 72 hours if required. The governing local law for SRS is California Civil Code § 1798.80 et seq; California Health & Safety Code § 1280.15; California Consumer Privacy Act of 2018.

**Commitment to the UK Data Protection Act (DPA)**
SRS is also committed to processing and securing data in accordance with the data protection principles of the Data Protection Act (UK, 1998), EU Data Protection Directive 95/46. SRS ensures that data is:

1. Processed fairly and lawfully
2. Obtained for limited purposes and not further processed in any manner incompatible with those purposes
3. Adequate, relevant and not excessive for the purposes for which they are processed
4. Accurate and up to date with ability for each company to update their data
5. Not kept for longer than is necessary
6. Processed in accordance with the data subject’s rights and preferences
7. Secure
8. Not transferred to other countries without adequate protection.
Information Collection and Use

Information Collected by SRS

SRS collects the data needed to provide accounts to SRS customer and supplier users in order to communicate with them. This data includes the contact information normally found on standard business cards, such as name, email, job title and telephone. SRS may use your email address to send you Service-related notices and announcements. No sensitive Personal Data is collected or stored.

Supply Risk Solutions (SRS) also collects and stores company and site assessment information and documents, and associated information.

Cookies and Log Data

SRS uses technologies like cookies and pixel tags to provide, monitor, analyze, promote and improve the Service. Server logs may include information such as user web requests, Internet Protocol (“IP”) address, user location, browser type, referring / exit pages and URLs, number of clicks and how you interact with links on the Service, domain names, landing pages, pages viewed, mobile carrier, and other such information. Log files help SRS to monitor, fix and improve the Service. When you access the Service using a mobile device, SRS may collect specific device information contained in your mobile device’s device identifier. SRS may associate this device identifier with your Service account and use data associated with your device identifier to tailor Services to your device and to analyze any device-related issues. Some web browsers have a “do not track” feature that lets you tell websites that you do not want to have your online activities tracked. SRS currently does not respond to “do not track” signals.

Links to Other Web Sites

SRS is not responsible for the practices employed by websites linked to from within the Service (e.g. news links), nor the information or content contained therein. Please remember that when you use a link to go from the Service to another website, our Privacy Policy is no longer in effect and your activities on that third party website is subject to such third party website’s own rules and policies.

ALL SRS SOFTWARE, INFORMATION, DOCUMENTATION, REPORTS, RECOMMENDATIONS, ADVICE, SERVICES, ETC. IN ANY MEDIA ARE PROVIDED ON AN “AS IS”, “AS AVAILABLE” BASIS. SRS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF ACCURACY, COMPLETENESS, AVAILABILITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORTS, LACK OF NEGLIGENCE OR NON-INFRINGEMENT. SRS INTELLECTUAL PROPERTY INCLUDES BUT IS NOT LIMITED TO SRS SERVICES, DATA, SOFTWARE, ETC. AND REMAINS EXCLUSIVE PROPERTY OF SRS. SRS IS GOVERNED BY THE LAWS OF SAN
MATEO COUNTY, CALIFORNIA, USA. PRIMARY AND BACKUP DATA CENTERS ARE LOCATED IN THE USA.

You agree to this Privacy Policy by accessing or using the Service.

Supply Risk Solutions (SRS) is the “Doing Business as” name for Accelor Corp, which was incorporated in California in January 2000.

SRS is committed to providing a secure, permission-controlled environment to support supply chain management. Revisions to the policies in this document will be dated and posted on this website. Please email any questions to bcmSupport@SupplyRisk.com. This document was last updated on May 2, 2019.