Supply Risk Solutions

Privacy and Security Policy

Privacy Certification

This Supply Risk Solutions (SRS) Privacy and Security Policy describes SRS' practices regarding the collection, 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"). The SRS Service improves customer-supplier business communications, business practices and transparency.

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), per Supplemental Principle 6 (Self-Certification), under the FTC's jurisdiction, effective July 25, 2016 forward. This commitment is backed by US law and is subject to the investigatory and enforcement powers of the US Federal Trade Commission (FTC).

SRS provides:

1. **Notice**: Inform data subjects via detailed online "privacy policy"
2. **Choice**: Offering option for data subjects to opt out of any direct marketing or use for other than the stated purpose with regard to data processing
3. **Security**: Appropriate security measures to safeguard personal data
4. **Data Integrity**: Personal data will be limited to what is relevant for the purpose of the processing, accurate, complete and current
5. **Access**: Data subjects can obtain confirmation of whether SRS processes personal data related to them, and, if so, be given the opportunity to correct, amend or delete personal data
6. **Accountability to Onward Transfers**: If SRS, wishes to transfer personal data to other data processors, SRS will ensure that the transfer is made on the basis of a contract which provides the same level of protection as the one guaranteed by the Privacy Principles. 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
7. **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, complaints or questions to SRS' CEO Patrick Brennan at bcmsupport@supplyrisk.com. SRS will normally reply within a few business days
- Independent Recourse Mechanism: An individual ("Data Subject") also has the option to seek recourse through an independent organization named JAMS (https://www.jamsadr.com/eu-us-privacy-shield). 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)

Additional Privacy Commitment

In addition, SRS is 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. 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 suppliers and customers 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.

SRS views collected data only as necessary to

- Maintain, provide and improve the Service
- Resolve a support request from you
- Comply with SRS customer agreements and Statements of Work
- Comply with or avoid the violation of applicable law, regulation or subpoena
- Better understand the manner in which our Service is being used.

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

Information Collection and Use

Information Collected by SRS

SRS collects the data needed to provide accounts to SRS customer users and to their supplier contacts and 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 supplier company, site assessment and documents from suppliers, as well as supplier categories such as supplier type, division, etc. from SRS customers.

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.

Multi-Level Data Security

SRS is committed to data security. SRS has therefore implemented multi-level physical, procedural and technical safeguards in connection with the storage, processing and transfer of data. These safeguards include the use of state-of-the-art data centers protected 24x365 by guards, firewalls, hardened hardware and software, data encryption, data backup, server monitoring and security vulnerability testing.

Data Center Guarded 24x365. The SRS Data Center facility is secured 24x365 by on-site guards as well as state-of-the-art video and audio monitoring equipment. All persons entering the building are required to be registered and possess a proper pre-issued ID card. Access is granted only to the minimum set of authorized personnel.

Network Security. SRS uses advanced network security that includes firewalls, routers, database access, and network controls. Network access to the servers has been limited to only the specific ports required by our applications. Direct access to our database servers is not allowed from public address space, including Internet connections. 128 bit or 256 bit SSL (HTTPS) or SSH encryption is used for all data transfers over the internet.

Hardened Servers. SRS has implemented the critical security controls recommended by the operating system vendor to control unauthorized access to the operating system functions. SRS applies security service packs as they become available and follow the recommendations of the operating system vendor in setting the security controls of the system.

Only the minimum necessary server ports are available, with all other ports are closed by default when a server is configured. Non-standard port numbers are assigned for the open ports. Only the operating system features that are needed for each server are installed in order to reduce the operating system attack area. Removable storage is never attached to the servers and server media is destroyed when no longer in use. Database information and backups are stored

Hardened Software Applications. SRS guards against common attack vectors and tests its software for application security. Each user is assigned a unique user name and password to access their data. SRS software does not allow any access to data without proper identification and authentication of the user. User session information is not passed in URLs or cookies. Instead, random session GUIDs are generated and refer to session objects on the server with a fixed expiration. All entered values must pass through HTML and URL encoding procedures.

Data Backups. SRS backs up data hourly off-site to a separate data center hundreds of miles away on servers that are not accessible to external personnel using the internet. This practice help prevent data loss and aids data recovery.

Servers and Software Monitored 24x365. The Network Operations Center monitors the servers and is staffed onsite 24x365. Servers are also monitored constantly by a leading host-based intrusion detection system (HIDS). Monitoring includes log analysis, integrity checking, registry monitoring, rootkit detection, time-based alerting and active response. Server event logs are logged redundantly to a separate server for independent analysis.

Vulnerability Tests. SRS conducts vulnerability assessments quarterly and after significant data center changes.

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 July 27, 2016.