



SuperLogics Intellectual Property Protection Policy

Document Owner: SuperLogics Management

Applies To: SuperLogics Incorporated

Document Type: Customer-Facing Policy Summary

Version: 2.0

Effective Date: 07/22/2026

1. Purpose

SuperLogics is committed to protecting the intellectual property, confidential information, technical data, and proprietary business information entrusted to us by our customers, suppliers, and business partners.

This policy summarizes SuperLogics' general approach to handling and protecting sensitive information received in connection with quoting, purchasing, manufacturing, configuration, testing, shipping, technical support, and related business activities.

2. Scope

This policy applies to information received, created, processed, stored, or used by SuperLogics in the course of normal business operations.

Examples include:

- Customer drawings, specifications, and technical requirements
- Bills of material and approved component lists
- Custom system configurations
- Purchase orders, forecasts, pricing, and delivery schedules
- Product requirements and performance specifications
- Software images, scripts, firmware, or configuration files
- Test procedures, quality records, and failure-analysis information
- Customer names, contacts, project details, and end-user information
- Supplier pricing, lead times, quotes, and sourcing information
- NDA-protected or otherwise confidential information
- Export-controlled, defense-related, or government-sensitive technical data, where applicable

This policy applies regardless of format, including electronic files, emails, paper documents, drawings, labels, photographs, test records, verbal communications, and production documentation.

3. General Policy Statement

SuperLogics handles customer and partner intellectual property with care and uses such information only for legitimate business purposes.

Customer-provided information is used only as necessary to support activities such as:

- Preparing quotations
- Processing orders



- Purchasing required materials
- Building and configuring customer systems
- Performing inspection, quality control, and testing
- Providing technical support
- Coordinating shipment and logistics
- Meeting applicable contractual, quality, or compliance requirements

SuperLogics does not sell, disclose, or intentionally share customer intellectual property or confidential information with unauthorized third parties.

4. Need-to-Know Access

Access to customer intellectual property and confidential information is limited to SuperLogics personnel who have a legitimate business need to use the information.

Examples of personnel who may require access include sales, purchasing, production, quality control, shipping, technical support, accounting, and management personnel involved in supporting the customer's order or business relationship.

SuperLogics personnel are expected to handle sensitive information responsibly and to avoid unnecessary copying, forwarding, printing, photographing, or distribution.

5. Customer Confidential Information

SuperLogics treats customer-specific information as confidential when it is marked confidential, provided under an NDA or similar agreement, subject to customer flow-down requirements, or reasonably understood to be non-public or sensitive.

Customer confidential information may include:

- Custom configurations
- System designs
- Technical specifications
- Drawings and schematics
- Program or project names
- End-customer information
- Pricing and purchase history
- Delivery schedules
- Forecasts
- Product-use information
- Test or inspection requirements

SuperLogics uses customer confidential information only to support the applicable customer relationship and related business activities.

6. Protection of Customer Designs and Configurations

Customer-provided designs, specifications, drawings, configuration requirements, and technical materials are used only for the purpose for which they were provided.



SuperLogics does not knowingly disclose one customer's proprietary design, drawing, custom configuration, or project-specific requirement to another customer without authorization.

SuperLogics may rely on general manufacturing knowledge, component expertise, supplier availability, industry experience, and product compatibility knowledge gained through normal business operations. However, customer-specific proprietary information is not intentionally reused or disclosed in a manner inconsistent with confidentiality obligations or customer trust.

7. Supplier and Partner Information

SuperLogics also protects confidential information received from suppliers, distributors, manufacturers, and other business partners.

This may include supplier pricing, product roadmaps, availability information, technical documents, account terms, and sourcing information.

Supplier or partner confidential information is not disclosed externally unless authorized or required for a legitimate business purpose.

8. Data Storage and Transmission

SuperLogics uses company-approved systems and business processes to store, transmit, and manage customer and partner information.

Personnel are expected to use care when transmitting sensitive information electronically, including verifying recipients before sending emails, attachments, shared files, or other communications.

SuperLogics avoids unnecessary distribution of sensitive information and limits access to those with a business need.

9. Physical Document and Production-Area Controls

Paper documents, drawings, labels, purchase orders, packing slips, work instructions, test records, and other production materials containing customer information are handled with reasonable care.

SuperLogics takes practical steps to reduce unnecessary exposure of customer information in production, assembly, testing, and shipping areas.

Visitors, vendors, or other third parties are not permitted to access customer confidential information, production records, customer-specific systems, or sensitive materials unless authorized.

Photography or video in production areas may be restricted when it could capture customer systems, labels, serial numbers, drawings, work instructions, or other sensitive information.

10. External Disclosure

SuperLogics does not disclose customer intellectual property or confidential information to outside parties unless there is a legitimate business purpose and the recipient is authorized to receive the information.

Examples of permitted business purposes may include:

- Coordinating with suppliers for component availability or technical compatibility
- Working with freight carriers or logistics providers
- Supporting warranty, repair, or technical service activity



- Meeting customer-approved quality or compliance requirements
- Responding to lawful or contractual obligations

Where appropriate, SuperLogics limits the information shared to what is necessary for the specific business purpose.

11. Public Communications and Marketing

General identification of a business relationship — such as referring to a company as a customer or business partner — is not considered disclosure of confidential information under this policy, provided the customer has not requested confidentiality, does not have an applicable non-disclosure or confidentiality agreement restricting such disclosure, and has not otherwise indicated that the relationship should not be publicly referenced.

SuperLogics does not publicly disclose customer-specific project details, order information, system configurations, photographs of customer systems, case studies, testimonials, or other customer-specific information unless authorized by the customer.

This applies to disclosure through websites, marketing materials, social media, trade-show materials, press releases, presentations, or customer references.

12. Export-Controlled or Restricted Information

Some customer technical information may be subject to export-control laws, defense-related restrictions, government flow-down requirements, or special handling requirements.

When SuperLogics is made aware that customer information is controlled, restricted, or subject to special handling requirements, SuperLogics will review the requirement on a case-by-case basis to determine whether it can be supported given SuperLogics' current facilities, personnel, and certifications.

This policy does not represent that SuperLogics holds ITAR registration, a facility security clearance, CMMC certification, or other specific defense- or government-related accreditation. Where a customer's requirement exceeds SuperLogics' current capabilities or certifications, SuperLogics will communicate that limitation to the customer rather than represent compliance it cannot support.

Customers are responsible for clearly identifying any export-controlled, classified, controlled unclassified, defense-related, or otherwise specially restricted information provided to SuperLogics, and for confirming SuperLogics' capabilities are sufficient for their specific requirement before providing such information.

13. Passwords, Credentials, and Access Information

If customer credentials, passwords, license keys, certificates, remote-access information, or similar access information are provided to SuperLogics for an authorized support purpose, SuperLogics handles that information with heightened care.

Such information is used only for the authorized purpose and should not be shared with unauthorized parties.

14. Incident Reporting and Response

If SuperLogics becomes aware of a suspected unauthorized access, disclosure, loss, theft, misuse, or mishandling of customer intellectual property or confidential information, SuperLogics will review the matter and take appropriate action based on the circumstances.



Potential actions may include containment, internal review, corrective action, customer communication, and process improvement.

15. Customer-Specific Requirements

Customers with specific intellectual property, confidentiality, cybersecurity, export-control, government, or flow-down requirements should provide those requirements to SuperLogics for review.

SuperLogics evaluates customer-specific requirements on a case-by-case basis to determine whether they can be supported.

16. Limitations

This policy is intended as a general customer-facing summary of SuperLogics' intellectual property protection practices. It does not disclose confidential internal security architecture, detailed system configurations, passwords, access-control details, or other sensitive operational information.

This policy does not create additional contractual obligations unless specifically incorporated into a written agreement signed by SuperLogics.

17. Summary Statement

SuperLogics maintains practical policies and procedures intended to protect customer intellectual property, confidential information, technical data, and proprietary business information. SuperLogics limits access to sensitive information based on business need, uses customer-provided information only for authorized business purposes, and expects personnel to protect such information from unauthorized use or disclosure.