Colony Brands, Inc.

Supply Chain Security Profile
Customs-Trade Partnership against Terrorism

Supplier Questionnaire

Colony Brands, Inc. (f/k/a The Swiss Colony, Inc.) is a member of the Customs-Trade Partnership against Terrorism (C-TPAT). This program is a key anti-terrorism initiative developed by U.S. Customs and Border Protection (CBP). As a C-TPAT member, Colony Brands must ensure that minimum-security procedures are in place throughout our supply chain. For purposes of C-TPAT, CBP defines the supply chain to extend from the point of origin (manufacturer/supplier/vendor) through to our distribution points in the United States.

We are required to have written and verifiable processes for the selection of business partners including manufacturers, product suppliers and vendors. As part of these processes, we must require you to demonstrate that your company's security procedures meet the minimum-security requirements established by U.S. Customs and Border Protection. Your responses to this questionnaire will help us meet our obligations as members of C-TPAT. Your responses will also help us obtain the benefits of the C-TPAT program, which include a reduced number of inspections when our goods arrive in the U.S.

Your responses and your compliance with the C-TPAT minimum-security criteria are subject to verification by us. We will incorporate the verification into our quality control and social compliance inspections of your facilities. I ask that the questionnaire be completed and returned to me within 30 days.

Please contact me before answering the questionnaire if you have any questions about the minimum-security procedures outlined in this questionnaire. The questionnaire is designed to identify those areas where improvements are needed to meet the minimum-security requirements. The correct identification of a security weakness will not adversely affect our business relationship but will enable us to work with you to develop a security improvement plan.

You must complete a questionnaire for each facility or location where you manufacture and ship goods to us. You may photocopy this questionnaire as needed. The questionnaire must be signed by an officer of the company. We require an updated form from every factory on a yearly basis.

Thank you,

AJ Schuchart
Sr. Manager, Global Logistics
Colony Brands, Inc. (f/k/a The Swiss Colony, Inc.)
Ph: 608-324-5094
Fax: 866-442-6604
Email: AJ.Schuchart@ColonyBrands.com

Name and Address of Facility:

_____

_____

_____

Container Security	Yes	No
1. Do you verify the physical integrity of the container structure prior to stuffing or loading? The inspection of the container is intended to identify the presence of false walls or other tampering with the container designed to facilitate unauthorized access to the container after it leaves your facility.	☐	☐
2. Does the inspection of the physical integrity of the container examine the following seven-points of the container's structure to ensure they have not been modified to conceal contraband or have been contaminated with agricultural pests? (Please answer questions 3-9)	☐	☐
3. Front wall (to detect any false walls and if applicable the fan housing on refrigerated containers)	☐	☐
4. Left side	☐	☐
5. Right side	☐	☐
6. Floor	☐	☐
7. Ceiling/Roof	☐	☐
8. Inside/outside doors (including the reliability of the locking mechanisms of the doors, handles, rods, hasps, rivets, brackets, and all other parts of a containers locking mechanisms)	☐	☐
9. Outside/undercarriage	☐	☐
10. After the container is stuffed or loaded do you affix a seal to the container?	☐	☐
During the container inspection process, do you use a checklist to show the following: (Please answer questions 11-15)		
11. Container / Trailers # / IIT (Instrument of International Traffic)	☐	☐
12. Date of Inspection	☐	☐
13. Time of Inspection	☐	☐
14. Name of the employee conducting the inspection	☐	☐
15. Specific areas of the IIT that were inspected	☐	☐
16. Does a supervisor sign off on the checklist when the inspection is completed?	☐	☐
17. Does the seal meet or exceed the PAS ISO 17712 standards for high security seals?	☐	☐

18. Who provides the seals to you?		
19. Do you maintain an inventory of seals? If yes, please answer question 20-21, if no please skip to question 22.	☐	☐
20. Do you record the seal numbers in a written record upon receipt of a new shipment?	☐	☐
21. When seals are used, do you record seal numbers with the container numbers on a written log, on the shipping documents, and on your internal records?	☐	☐
22. Do you have written procedures to control access to the seals?	☐	☐
23. Do you have written procedures regarding the correct method to affix the seal to the container?	☐	☐
24. Do you take digital pictures of the properly installed seal at the point of stuffing and share them with the consignee for verification purposes?	☐	☐
25. Do you conduct a periodic audit of the stored seals and reconciliation against seal inventory logs and shipping documents? All audits must be documented.	☐	☐
26. Do you store containers in a secure area to prevent unauthorized access and/or tampering?	☐	☐
27. Do you have written procedures to report unauthorized entry into containers or container storage areas to local law enforcement officials?	☐	☐
Physical Security		
28. Are all buildings constructed of materials that resist unlawful entry and protect against outside intrusion?	☐	☐
29. Are cargo handling and storage facilities enclosed by fencing?	☐	☐
30. Are the gates, through which vehicles enter cargo handling and storage facilities manned and/or monitored at all times when the facility is open?	☐	☐
31. Do you have a policy that notifies individuals that they and their vehicles may be subject to search in accordance with local and labor laws?	☐	☐
32. Are the entrance gates closed and locked when the facility is closed?	☐	☐
33. Do you have written procedures to report unauthorized entry into the facility to local law enforcement officials?	☐	☐
34. Do you use video surveillance cameras to monitor the entrances to the facility and the cargo handling and storage / inspection areas? If yes, please answer question 35. If no, please skip to question 36.	☐	☐
35. Do you store the tapes for a period of time before reusing them? If yes, how long (90-120 days)?	☐	☐

36. Do you have periodic, random reviews of the camera footage to verify that cargo security procedures are being properly followed and maintained for a minimum of 2 years for audit purposes?	☐	☐
37. Is the facility equipped with an alarm system to monitor the entrances to the facility?	☐	☐
38. Is there adequate lighting inside and outside the facility, including parking areas, fence lines, entrances and exits, and cargo handling and storage /inspection areas?	☐	☐
39. Are locking devices used to secure external and internal doors, windows, gates and fences?	☐	☐
40. Do management and/or security personnel control the issuance of keys?	☐	☐
41. Are employee / visitor vehicles prohibited from parking in or adjacent to cargo handling and storage areas?	☐	☐
42. Do you segregate high-value and/or dangerous cargo in a secure area within the warehouse or storage yard?	☐	☐
43. Do you have a communication system to contact internal security personnel and/or local law enforcement authorities?	☐	☐
44. Do you use Security Technology for physical security? If yes, please answer question 45-47, if no please skip to question 48.	☐	☐

45. Do you have written policies and procedures governing the use, maintenance, and protection of security technology?
These policies must:
  a. Limit access to the locations of controls / hardware for security devices;
  b. Procedures to test / inspect the technology on a regular basis;
  c. Inspections include verification that equipment is correctly positioned and/or working properly;
  d. Document the results of the inspections and performance testing;
  e. If corrective actions are warranted, implement and document the actions taken;
  f. Documented results must be maintained for a sufficient time for audit purposes.
	☐	☐

46. Do you have a written agreement with third-party (off-site) security monitoring resources in place, stipulating critical systems functionality and authentication protocols, such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revision(s), and systems access or denial(s)?	☐	☐
47. Are security technology policies and procedures reviewed at least annually and updated as risk circumstances change?	☐	☐
Access Controls		
48. Do you have an employee identification system which provides for the positive identification of employees before they can enter the facility?	☐	☐
49. Do employees have access only to those areas in which they perform their duties?	☐	☐

50. Do management and/or security personnel control the issuance of employee, visitor and vendor identification badges?	☐	☐
51. Are visitors required to present photo identification upon arrival?	☐	☐
52. Are visitors required to visibly display a temporary identification badge while on the premises?	☐	☐
53. Are visitors escorted at all times by company personnel while on the premises?	☐	☐
54. Are vendors and other delivery personnel required to present photo identification upon arrival?	☐	☐
55. Are arriving packages and mail periodically screened before delivery within the company?	☐	☐
56. Do you have identification procedures for all employees, visitors and vendors at all points of entry?	☐	☐
57. Do you have written policies and procedures for security guards and periodically verify compliance with these work instructions and policies through audits, policy reviews, and simulated exercises?	☐	☐
58. Do you have procedures to challenge unauthorized/unidentified persons and to report problems to local law enforcement officials?	☐	☐
Procedural Security		
59. Do you have a designated security officer to supervise the loading of cargo into containers, trailers and railcars?	☐	☐
60. Do you verify the quantity and identity of goods against the purchase order prior to shipment?	☐	☐
61. Do you have procedures to resolve discrepancies prior to shipment?	☐	☐
62. Do you track the timeliness of incoming and outgoing cargo movements?	☐	☐
63. Do you maintain a written log recording the identity of the driver, positively identifying the driver, and the container number of the cargo picked up?	☐	☐
64. Do you have procedures to ensure that all information related to our orders is protected against loss or the introduction of erroneous information?	☐	☐
65. Do you have procedures to ensure that all shipping documents are legible, complete and accurate?	☐	☐
66. Are your computer systems and the information stored on them protected against unauthorized access?	☐	☐
67. Do you have procedures to notify U.S. Customs and/or local law enforcement officials when anomalies or illegal activities are suspected?	☐	☐

68. Do you have a statement of support to protect your supply chain from criminal activities such as drug trafficking, terrorism, human smuggling and illegal contraband that is it signed by a company official and displayed on company bulletin boards?	☐	☐
69. Do you have a Supply Chain Security Program that includes many departments, such as Security, Human Resources, Information Technology and Import/Export offices to create a cross-functional team focused on your company's Supply Chain Security?	☐	☐
70. Do you have a multi-level audit system, in verifiable format, that tests your security programs with checks, balances and accountability in mind to ensure the program operates as planned?	☐	☐
71. Do you have written procedures in place that addresses crisis management, business continuity, security recovery plans and business resumption?	☐	☐
72. Do you have written procedures to separate and secure domestic cargo from International cargo in warehouse or pre-staging areas?	☐	☐
73. Do you inspect cargo staging areas, and the immediate surrounding areas on a regular basis to ensure these areas remain free of visible pest contamination?	☐	☐
74. Do you have written procedures to prevent pest contamination & include Wood Packaging Materials (WPM) regulations under the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No, 15 (ISPM 15)?	☐	☐
Information Technology Security		
75. Do you use individually assigned accounts for personnel to access your information technology systems based on job requirements?	☐	☐
76. Do you require users to periodically change the passwords used to access your information technology systems?	☐	☐
77. Do you use firewalls to protect your information technology systems from unauthorized access from the internet?	☐	☐
78. Do you have a system to identify the abuse of your information technology systems including the improper access, tampering or altering of business data?	☐	☐
79. If using a network system, do you regularly test the security of your IT infrastructure?	☐	☐
80. Do you have policies and procedures on Cybersecurity, and do they address how information is shared based on cybersecurity threats with the Government and other business partners on an annual basis?	☐	☐
81. Do you allow your personnel to connect remotely to your network via a virtual private network (VPN)? If yes, please answer question 82, if no, skip to question 83.	☐	☐
82. If you use a VPN, do you have procedures designed to secure remote access from unauthorized users?	☐	☐
83. Do you allow employees to use personal devices to conduct company work? if yes, please answer question 84, if no, skip to question 85.	☐	☐
84. If you allow employees to use personal devices to conduct company work, do you have policies and procedures to include regular security updates and a method to securely access the company's network?	☐	☐

85. Do your cybersecurity policies and procedures include measures to prevent the use of counterfeit or improperly licensed technological products?	☐	☐
86. How often is your data backed up and is your data stored in an encrypted format offsite of your facility? _____		
87. Do you regularly account for your IT inventory and is it properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines?	☐	☐
Personnel Security		
The following personnel security procedures must be followed in accordance with local laws and regulations.		
88. Do you conduct pre-employment screening and background checks on prospective employees?	☐	☐
89. Do you verify the information provided by job applicants, including employment history and references?	☐	☐
90. Do you have procedures to report and manage problems related to personnel security?	☐	☐
91. Do you periodically conduct background checks on current employees based on cause and/or the sensitivity of the employee's position?	☐	☐
92. Do you have procedures to remove identification badges and to deny facility and information systems access for terminated employees?	☐	☐
Employee Education and Awareness		
93. Do you have or plan to have a security awareness program to educate employees to recognize internal conspiracies, maintain cargo integrity and to identify and address security issues?	☐	☐
94. Does the security awareness program encourage and reward employees for active participation in security programs?	☐	☐
95. Do you require personnel who operate and manage security technology systems to have received specialized training on the system's operation and maintenance?	☐	☐
Threat Awareness		
96. Do you have or plan to have a threat awareness program established and maintained by security personnel and designed to recognize and foster awareness of the threat posed by money laundering and terrorism financing activities?	☐	☐
Verification		
97. Are the specific procedures identified in this questionnaire response maintained in a verifiable format?	☐	☐
98. Have you obtained a certification in a supply chain security program by a foreign Customs Administration?	☐	☐

If so, please provide your status of participation here and include a copy of your certificate with your response to this questionnaire.		

Name of Person Completing or Supervising the Completion of the Questionnaire:

_____

Name and Title

_____

Date

_____

Signature

Please email or fax the completed form to:

GlobalCompliance@ColonyBrands.com (Email)

or

800-420-1356 (Fax)