Supply Chain Audit for C-TPAT and General Compliance Program
Manufacturer's Audit Form

Factory Name: CHAOZHOU LUYUAN FOOD INDUSTRIAL CO., LTD NO.1 BRANCH FACTORY 潮州市潮安区绿园食品实业有限公司第一分厂 **Company Name:** Tai Sam (Party Fun) Ind. Co. Ltd	**Auditor's Assessment:** Pass: ☑ Fail: □
Unique Factory Code: 66	
Factory Address: West Po District, Dragon Pit Village, Anbu Town, Chaoan Area, Chaozhou City, Guangdong Province, China 中国广东省潮州市潮安区庵埠镇龙坑村西埔片	
Phone Number: 86+768-6670067	
Fax Number: N/A	
Primary Contact: Kat Tang	
Title of Contact: Secretary	
E-Mail of Contact: kat@taisam.com.hk	
Audit Date: Nov 16-17, 2020	
Name of Auditor: Sam Luo	
Report Number: 188	
Report Date: Nov 17, 2020	

Audit Score (Total of "Yes" and "N/A" Answers):

□	**85 – 130**	**Certified Manufacturer: 5 Year Exemption**
☑	**60 – 84**	**Certified Manufacturer: 3 Year Exemption**
□	**59 and Below**	**Non-Certified Manufacturer: Must Achieve Score of 60**

Manufacturer must respond in writing to all points of the Corrective Action Plan (CAP) within sixty (60) days of the date of this Report. If the Manufacturer does not respond within 60 days with a written commitment to improve and proof of Corrective Action (where requested), the Manufacturer shall *fail*, Certification shall be denied, and the Manufacturer shall no longer be a supplier for Unique.

See "Part 7 – Conclusion" For Your Company's Requirements

Type of Audit (Check Box Below)

	Initial Audit		
Yes	Follow-Up Audit	Prior Report #:	172
	Other Audit (Please specify):	Prior Report Date	Aug 15 2019
The findings in this Audit are intended to be confidential and proprietary business information of Unique Industries, and are obtained for C-TPAT compliance purposes. The above reflects the findings for the particular manufacturer identified on the date of the Audit only. This report does not certify or imply: (a) compliance with any government, industry, or association regulations or standards; (b) the quality of any specific products manufactured (if any); or (c) the shipment of any specific products. This report does not discharge or release the manufacturer from its commercial, legal or contractual obligations with Unique Industries or its affiliated or related entities.			

Part 1 – Instructions: An Auditor has been instructed to visit the Manufacturer’s facility. The Auditor will verify the answers to the questions set forth in the Questionnaire, found in Part 2 below.

- A “Yes” answer means that the Auditor has verified that the answer to the question is *yes*.
- A “No” answer means that the Auditor has verified that the answer to the question is *no*, or has *not been able* to verify the answer.
- A “N/A” answer means that question is *not applicable* to this manufacturer.
- The words “verification” or “verify” means that the manufacturer must *prove to the Auditor* that the answer given by the manufacturer is true. The Auditor must review documents, conduct interviews, witness procedures and inspect the facility, all in an effort to confirm that what this manufacturer represented is true.

Part 2 – Questionnaire: Please answer the questions below in the presence of the Auditor. If the manufacturer answers “Yes” or “N/A” to any question, the manufacturer must provide verification to the Auditor.

A.	**General**	**Yes**	**No**	**N/A**
1.	Unique Industries, Inc. (“Unique”) partnered with U.S. Customs in C-TPAT, a U.S. Customs-based initiative designed to strengthen supply chain security. Will your company agree to work with Unique and U.S. Customs to strengthen and increase supply chain security?	√		
B.	**Personnel Security**			
2.	Are potential employees required to fill out an application for employment and present a photo ID card prior to hiring?	√		
3.	Are potential employees interviewed by someone from your company?	√		
4.	Does your company conduct criminal investigations for permanent employees prior to their employment?		√	

5.	Does your company conduct background investigations for permanent employees prior to their employment?		√	
6.	Are alternative measures used to check potential employees' backgrounds if they live or work in jurisdictions prohibiting background checks?		√	
7.	Are re-investigations conducted for permanent employees?		√	
8.	Are potential employees required to undergo drug and alcohol screening?			√
9.	Are personnel records like documents 2 through 8 maintained in individual permanent files?	√		
10.	Do you maintain permanent employee files which contain the results of background investigations, application and interview materials, drug and alcohol screening results, and disciplinary issues concerning employees?	√		
11.	Do you maintain permanent employee and temporary (contract) employee files which include employee names, addresses, birthdates, photo identification, identification numbers (example: national identification number, social security), and position?	√		
12.	Do you have a written policy that requires the issuance of access credentials (ID badge or access cards) to every permanent (full-time and part-time) and temporary (contract) employee?	√		
13.	Do you have written procedures and/or a checklist in place to take back employee identification, revoke facility and system access, deny physical access, and obtain company property from terminated employees?	√		
14.	If 'yes' to preceding question, are managers given periodic training to ensure that these procedures are consistently followed?		√	
15.	Do you have a written Code of Conduct which specifies what is considered a breach of company security, as well as an outline of resulting disciplinary actions?		√	
16.	Are employees educated about company security policies and procedures prior to their formal employment with your company?		√	
17.	Is a list of names and/or photo system updated and utilized to aid in controlling the access by terminated employees?	√		
18.	Are your personnel/employee policies in writing, periodically assessed to ensure compliance, and updated as necessary?		√	
19.	Do your personnel/employee policies and documented procedures cover employee hiring, personnel records systems, and employee screening processes?	√		
20.	Do your personnel/employee policies instruct your employees on how to manage such policies?	√		
21.	Do you have a documented procedure to perform background checks?	√		
22.	Do you have a written procedure to review the background check of sensitive positions?	√		

23.	Do you have a written employee termination policy?	√		
C.	**Procedural Security**			
24.	Do you have procedures in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous (wrong/false) information?	√		
25.	Do you have procedures in place for retaining and safeguarding physical documents and computer files related to merchandise/cargo information?	√		
26.	Do you have procedures in place for notifying the appropriate law enforcement agencies when security breaches, tampering, or illegal activities are detected or suspected?	√		
27.	Are employees trained to identify a list of "suspicious activity" indicators?	√		
28.	If yes to the preceding question, do you keep a record of the employees who attended the training?	√		
29.	Do you have tracking procedures for monitoring the transportation of cargo?	√		
30.	Do you have procedures for recording and investigating shortages/overages incidents?	√		
31.	Do you have procedures to verify that cargo weights, labels, marks, and piece counts are verified?		√	
32.	Do you have a procedure for monitoring goods within your warehouse to prevent tampering?	√		
33.	Do you have a policy for retaining physical records and computer data?		√	
34.	Is access to data, records, and other business matter controlled and safeguarded from unauthorized use?		√	
35.	Do you have procedures for securing and isolating dangerous items and contraband, and do those procedures include notifying the appropriate governmental agency?	√		
36.	Are all of these Procedural Security policies documented, periodically assessed to ensure compliance, and updated if necessary?		√	
37.	Do you have restricted or sensitive areas?	√		
38.	If yes, do you have a written policy regarding access controls to restricted or sensitive areas?	√		
39.	Do you review and update employee lists that authorize access to sensitive or restricted work areas?		√	

40.	Do you maintain records of security guard reports, security guard patrols, or other incident reports?		√	
41.	Do you have a written policy/procedure requiring that security incidents are reported, logged and investigated?		√	
42.	Do you conduct a regular review of shipment information and documentation controls to verify accuracy and security?		√	
43.	Do you have a “designated zone” (with frame and lock) for security sensitive areas?	√		
D.	**General Physical Security**			
44.	Are your buildings and related facilities constructed of materials which resist unlawful entry?	√		
45.	Do you have perimeter gates, fences, or other barriers?	√		
46.	Are private vehicles prohibited from parking near cargo storage and loading areas?		√	
47.	Do you have locks which prevent unauthorized access to internal and external doors, windows, gates, and fences?	√		
48.	Is your facility well-lit on the inside and outside?	√		
49.	Do you have an internal security department or use an outside security company to guard your facilities?	√		
50.	Do you have more than one guard per shift?		√	
51.	Do you have an alarm system at your facilities?		√	
52.	Do you have a surveillance camera (closed-circuit television) system at your facilities?	√		
53.	If yes to the preceding question, do you preserve video records for at least forty-five (45) days?		√	
54.	Do you or a third party inspect and maintain the physical security items identified above? If yes, are records kept to show inspections and repairs?		√	
55.	Do you have physical security policies that are communicated to each employee?		√	
56.	Is there a written policy that requires security procedures to be documented as a policy or procedure?	√		
57.	Are these written policies periodically assessed via a written report to ensure compliance, and updated if necessary?		√	
58.	Do you keep and maintain security meeting records and emergency contact lists?	√		
E.	**Physical Access Security**			

59.	Do you require photo identification or use another system to identify employees?	√		
60.	Do employees gain entrance to the facility through a secure point of entry using keys, access cards, photo identification, security guard checkpoints, or similar methods?	√		
61.	Is there a written key control and access card log that keeps track of who has keys/cards and what the keys/cards open or access?	√		
62.	Is the issuance of photo identification and access materials controlled, recorded and supervised by at least one designated employee?	√		
63.	Is there a written procedure requiring employees and visitors to show photo identification prior to entering your facility?	√		
64.	Do you maintain a sign-in/sign-out log for visitors indicating the following information: first and last name, company affiliation, phone number, badge number, entrance and exit times, purpose of visit, and the employee whom they are visiting?	√		
65.	Is there a written policy requiring visitors to wear identification badges while at your facility?	√		
66.	Is there a written policy requiring visitors to be escorted by at least one of your employees while inside your facilities?	√		
67.	Do you have procedures in place for identifying, challenging, and addressing unauthorized/unidentified persons?		√	
68.	Are employees given access only to those secure areas needed for the performance of their duties?		√	
69.	Do you have standard written physical access policies that are communicated to each employee?	√		
70.	Are these policies periodically assessed to ensure compliance and updated if necessary?		√	
71.	Do you have a written program to perform security and maintenance inspections of buildings, based on risk?	√		
72.	Do you maintain records of building inspections?	√		
73.	Do you have a written policy and procedure for security meetings?	√		
F.	**Information Technology Security**			
74.	Do you have an internal system to restrict access to individual computers, such as password assignments?	√		

75.	Do you have an internal system to restrict access to the main system server?		√	
76.	Do you have a system for monitoring and limiting the access of the internet and/or other programs to which only permitted employees are allowed access?	√		
77.	Do you use anti-virus software?	√		
78.	Do you have a firewall protection program?	√		
79.	Do you have a disaster recovery system to recover lost or stolen data?		√	
80.	Are Information Technology security policies, procedures and standards in place?		√	
81.	Are your company's employees trained on the Information Technology security policies, procedures and standards in place?	√		
82.	Are information technology policies that are addressed to employees documented in writing and assessed periodically to ensure compliance?		√	
83.	Are employees who violate Information Technology policies subject to disciplinary action?	√		
84.	Do you have your system administrator receive a report of invalid password attempts?	√		
G.	**Container/Trailer/Conveyance Security**			
85.	Are containers/trailers retained at your facility overnight?			√
86.	If so, are they re-inspected prior to loading or shipping?			√
87.	Does your company, or a company loading the container, inspect the container and perform the seven-point inspection found in Unique's "Pre-Loading Container Inspection Certificate & C-TPAT Status" Memorandum prior to loading a container?	√		
88.	Does your company maintain records of the seven-point inspections?	√		
89.	If containers (full or empty) are stored at your facility, do you employ safety measures to prevent unauthorized access and/or manipulation?	√		
90.	If you own or operate your own equipment to transport product, do you have procedures for ensuring that only permitted employees and visitors have access to the equipment?		√	
91.	Are there written policies to log truck and container/trailer arrivals and departures which notes deliveries entering and exiting your facility?	√		

92.	Is there a written policy prohibiting personal items (such as a lunch box, backpack, etc.) in the packing and shipping areas?		√	
93.	Is the person responsible for overall security identified in writing?	√		
94.	Are procedures and policies in place to report and neutralize unauthorized entry into containers or container storage areas?	√		
95.	Are these procedures and policies documented in writing, periodically assessed to ensure compliance, and updated if necessary?		√	
96.	Do you maintain shipment records?		√	
97.	Do you maintain shipment records for no less than two (2) years?		√	
98.	Do you maintain records of shipment information and documentation to verify accuracy and security?		√	
H.	**Seals**			
99.	When sealing containers, does your company use high-security seals that meet or exceed current PAS ISO 17712 standards?	√		
100.	Do you have a written procedure showing how high security seals are to be affixed to a container, how they are to be recorded onto a usage log, and how they are to be tracked?		√	
101.	Do you maintain a seal control log?	√		
102.	Are security seals kept in a secured location, to prevent them from being tampered with?	√		
103.	Does your company control the issuance of seals by having one person, or a limited group of people, responsible for protecting and handling the seals?	√		
104.	Are new and unused security seal numbers kept in a written log and stored in a secure area which prevents unauthorized access to them?		√	
105.	Do you have procedures for verifying that seals on containers, trailers, and railcars are in good condition and have not been tampered with or broken?		√	
106.	If seal tampering occurs, do you have a procedure for investigating and retaining the seal until an investigation is complete?		√	
107.	Does your company identify which seal was used on which container?	√		

108.	Are security seal numbers verified at various stages along the supply chain?	√		
109.	Are these policies documented in writing, periodically assessed to ensure compliance, and updated if necessary?		√	
110.	Does your company keep and maintain records of the seal number and information, so that the seal could be tracked through the supply chain?	√		
I.	**Business Partner Requirements**			
111.	Do you require your vendors and/or business partners to adhere to a security Code of Conduct?	√		
112.	Do you have verifiable processes for the selection of business partners?	√		
113.	Do you address security issues with vendors and assist in taking measures to improve weaknesses in security?		√	
114.	Do you certify or audit a vendor’s facilities to assess security policies?		√	
115.	Are these policies documented in writing, periodically assessed to ensure compliance, and updated if necessary?		√	
116.	Do you have written contracts with your freight consolidators, logistics providers, and other transportation vendors?	√		
117.	Do your agreements include a process for drivers to report container security issues?	√		
118.	Do you have a written and implemented procedure regarding security vetting of service contractors who require routine or scheduled access to the facility?		√	
119.	Do you send out corrective action notices to vendors or subcontractors in the event they do something to violate your security policies or procedures?		√	
J.	**Security Training/Threat Awareness/Outreach**			
120.	Does your company have a security training and threat awareness program for employees?	√		
121.	Does your security program include training covering the recognition of internal conspiracies, the maintenance of cargo integrity, and the identifying and addressing of unauthorized access?	√		
122.	Do your new employee orientation procedure and training materials address the security procedures you have in place, how to address security breaches, and how to report them?	√		

123.	Do your training materials have specialized training for shipping and receiving employees which is recorded/documented?	√		
124.	Do you keep records of your new employee orientation procedure and training materials given to your employees?	√		
125.	Does your security program have a written procedure that requires the reporting of suspicious activities and security violations?	√		
126.	Does your security program include incentives for employees who take an operative role in security awareness?	√		
127.	Is your threat awareness program written down and published to all employees?		√	
128.	Is additional security training provided to employees in your company's shipping and receiving areas?		√	
129.	Is additional security training provided to employees responsible for receiving and opening mail?	√		
130.	Are these security training and threat awareness policies and procedures documented, periodically assessed to ensure compliance, and updated as necessary?		√	

Part 3 – Summary of Points: A manufacturer receives one (1) point for each "Yes" response, one (1) point for each "N/A" response, and zero (0) points for each "No" response.

Sections	**Maximum Points Available (130)**	**Points Achieved**
A – General	1	1
B – Personnel Security	22	14
C – Procedural Security	20	12
D – General Physical Security	15	8
E – Physical Access Security	15	12
F – Information Technology Security	11	7
G – Container/Trailer/Conveyance Security	14	8
H – Seals	12	7
I – Business Partner Requirements	9	4
J – Security Training/Threat Awareness/Outreach	11	8
	Total Points Achieved:	81

Part 4 – Remarks: Please make any remarks and comments necessary for any of the Questions found in the Questionnaire Section (Part 2) of this Audit:

Question No.	Remarks
4	No evidence that factory conducts criminal investigations for permanent employees prior to their employment.
5	No evidence that factory conducts background investigations for permanent employees prior to their employment.
6	No evidence that factory uses any alternative measures to check potential employees' backgrounds if they live or work in jurisdictions prohibiting background checks.
7	No evidence that re-investigations are conducted for permanent employees.
14	No evidence that managers are given periodic training to ensure that the procedures listed Q.13 is consistently followed.
15	No evidence that factory has physical security policies which are communicated to each employee.
16	No evidence that employees are educated about company security policies and procedures prior to their formal employment.
18	No evidence that personnel/employee policies are in writing, periodically assessed to ensure compliance, and updated as necessary.
31	No evidence that factory has procedures to verify the weights, labels, marks, and piece counts of cargo.
33	No evidence that factory has a policy for retaining physical records and computer data.
34	No evidence that factory controls the access to data, records, and other business matter and safeguard from unauthorized use.
36	No evidence that the Procedural Security policies are documented, periodically assessed to ensure compliance, and updated if necessary.
39	No evidence that factory reviews and updates employee lists that authorize access to sensitive or restricted work areas.
40	No evidence that factory maintains records of security guard reports, security guard patrols, or other incident reports.
41	No evidence that a written policy/procedure is required to report/log/investigate security incidents.
42	No evidence that factory conducts a regular review of shipment information and documentation controls to verify accuracy and security.
46	No evidence that private vehicles are prohibited from parking near cargo storage and loading areas.
50	No evidence that factory had more than one guard per shift.
51	No evidence that factory has an alarm system at facilities.
53	No evidence that factory preserves (CCTV) video records for at least forty-five (45) days.
54	No evidence that factory or any third party inspects and maintains the physical security items. No evidence that factory keeps the records for inspections and repairs.
55	No evidence that factory has physical security policies and communicates to each employee.
57	No evidence that written policies are periodically assessed via a written report to ensure compliance, and updated if necessary.
67	No evidence that factory has procedures for identifying, challenging, and addressing unauthorized/unidentified persons.

68	No evidence that employees are given access only to those secure areas needed for the performance of their duties.
70	No evidence that those policies are periodically assessed to ensure compliance and updated if necessary.
75	No evidence that factory has an internal system to restrict access to the main system server.
79	No evidence that factory has a disaster recovery system to recover loss or stolen data.
80	No evidence that Information Technology security policies, procedures and standards are in place.
82	No evidence that information technology policies that are addressed to employees is documented in writing and assessed periodically to ensure compliance.
90	No evidence that factory has procedures for ensuring that only permitted employees and visitors have access right to her own equipment for transporting product.
92	No evidence that there is a written policy prohibiting personal items (such as a lunch box, backpack, etc.) in the packing and shipping areas.
95	No evidence that those procedures and policies are documented in writing, periodically assessed to ensure compliance, and updated if necessary.
96	No evidence that factory maintains completed shipment records.
97	No evidence that factory maintains shipment records for no less than two (2) years.
98	No evidence that factory maintains records of shipment information and documentation to verify accuracy and security.
100	No evidence that factory has a written procedure showing how high security seals are to be affixed to a container, how they are to be recorded onto a usage log, and how they are to be tracked.
104	No evidence that new and unused security seal numbers are kept in a written log and stored in a secure area which prevents unauthorized access.
105	No evidence that factory has procedures for verifying that seals on containers, trailers, and railcars are in good condition and have not been tampered with or broken.
106	If seal tampering occurs, no evidence that factory has a procedure for investigating and retaining the seal until an investigation is complete.
109	No evidence that those policies are documented in writing, periodically assessed to ensure compliance, and updated if necessary.
113	No evidence that factory addresses security issues with vendors and assists in taking measures to improve weaknesses in security.
114	No evidence that factory certifies or audits vendor's facilities to assess security policies.
115	No evidence that those policies are documented in writing, periodically assessed to ensure compliance, and updated if necessary.
118	No evidence that factory has a procedure regarding security vetting of service contractors who require routine or scheduled access to the factory.
119	No evidence that factory sends out corrective action notices to vendors or subcontractors in the event they do something to violate security policies or procedures.
127	No evidence that the threat awareness program is written down and published to all employees.
128	No evidence that additional security training is provided to employees working in shipping and receiving areas.
130	No evidence that those security training and threat awareness policies and procedures are documented, periodically assessed to ensure compliance, and updated as necessary.

Auditor to Add Rows as Necessary

Part 5 – Related Notes:

List the name and title of each representative from the manufacturer who assisted the Auditor in responding to these questions:

Name/Title:	Lihui Zhao 赵立惠 / Sales Manager 业务部经理
Name/Title:	Bingchun Chen 陈冰纯/ Personnel Supervisor 人事部主管
Name/Title:	Jiansheng Rao 饶建生 / Security Captain 保安部队长
Name/Title:	Canhong Zhang 张灿宏 / Warehouse Supervisor 仓库部主管
Name/Title:	Ziyan Qiu 邱紫燕/ Packaging supervisor 包装部主管

Part 6 – Corrective Action Plan:

The Manufacturer must take the following corrective actions before the next Audit:

#	Actions
1	4. It is suggested that factory should conduct criminal investigations for permanent employees prior to their employment .
2	5. It is suggested that factory should conduct background investigations for permanent employees prior to their employment.
3	6. It is suggested that factory should find the alternative measures to check potential employees' backgrounds if they live or work in jurisdictions prohibiting background checks.
4	7. It is suggested that factory should conduct re-investigation to permanent employees.
5	14. It is suggested that factory should provide periodic training to managers to ensure that the procedures listed Q.13 is consistently followed.
6	15. It is suggested that factory should establish physical security policies which are communicated to each employee.
7	16. It is suggested that factory should provide training about company security policies and procedures to employees prior to their formal employment.
8	18. It is suggested that factory should make sure personnel/employee policies to be in writing, periodically assessed to ensure compliance, and updated as necessary.
9	31. It is suggested that factory should establish procedures to verify the weights, labels, marks, and piece counts of cargo.
10	33. It is suggested that factory should establish a policy for retaining physical records and computer data.
11	34. It is suggested that factory should control the access to data, records, and other business matter and safeguard from unauthorized use.
12	36. It is suggested that factory should make sure Procedural Security policies to be documented, periodically assessed to ensure compliance, and updated if necessary.

13	39. It is suggested that factory should review and update employee lists that authorize access to sensitive or restricted work areas.
14	40. It is suggested that factory should maintain and keep records of security guard reports, security guard patrols, or other incident reports.
15	41. It is suggested that factory should establish a written policy/procedure to report/log/investigate security incidents.
16	42. It is suggested that factory should conduct a regular review of shipment information and documentation controls to verify accuracy and security.
17	46. It is suggested that factory should make sure private vehicles to be prohibited from parking near cargo storage and loading areas.
18	50. It is suggested that factory should have more than one guard per shift.
19	51. It is suggested that factory should try the best to set up an alarm system at facilities.
20	53. It is suggested that factory should try the best to upgrade the hardware to preserves (CCTV) video records for at least forty-five (45) days.
21	54. It is suggested that factory should make sure to inspect and maintain the physical security items by their own or by any 3rd party. It is also suggested that they should keep the records for inspections and repairs.
22	55. It is suggested that factory should establish physical security policies and should communicate to each employee.
23	57. It is suggested that factory should make sure written policies to be periodically assessed via a written report to ensure compliance, and updated if necessary.
24	67. It is suggested that factory should establish procedures for identifying, challenging, and addressing unauthorized/unidentified persons.
25	68. It is suggested that factory should allow employees to access only to those secure areas needed for the performance of their duties.
26	70. It is suggested that factory should make sure the policies to be periodically assessed to ensure compliance and updated if necessary.
27	75. It is suggested that factory should set up an internal system to restrict access to the main system server.
28	79. It is suggested that factory should try the best to set up a disaster recovery system to recover loss or stolen data.
29	80. It is suggested that factory should make sure Information Technology security policies, procedures and standards to be in place.
30	82. It is suggested that factory should address information technology policies to employees and document in writing and assess them periodically to ensure compliance.
31	90. It is suggested that factory should establish procedures to ensure that only permitted employees and visitors have access right to her own equipment for transporting product.
32	92. It is suggested that factory should issue a policy prohibiting personal items (such as a lunch box, backpack, etc.) in the packing and shipping areas.
33	95. It is suggested that factory should make sure the procedures and policies to be documented in writing, periodically assessed to ensure compliance, and updated if necessary.
34	96. It is suggested that factory should maintain shipment records.
35	97. It is suggested that factory should maintain shipment records for no less than two (2) years.
36	98. It is suggested that factory should maintain records of shipment information and documentation to verify accuracy and security.
37	100. It is suggested that factory should establish a written procedure showing how high

	security seals are to be affixed to a container, how they are to be recorded onto a usage log, and how they are to be tracked.
38	104. It is suggested that factory should keep record/ log for new and unused security seal numbers and store them in a secure area which prevents unauthorized access.
39	105. It is suggested that factory should establish procedures for verifying that seals on containers, trailers, and railcars are in good condition and are not tampered with or broken.
40	106. If seal tampering occurs, it is suggested that factory should establish a procedure for investigating and retaining the seal until an investigation is complete.
41	109. It is suggested that the policies should be documented in writing, periodically assessed to ensure compliance, and updated if necessary.
42	113. It is suggested that factory should address security issues with vendors and assist in taking measures to improve weaknesses in security.
43	114. It is suggested that factory should certify or audit vendor's facilities to assess security policies.
44	115. It is suggested that the policies should be documented in writing, periodically assessed to ensure compliance, and updated if necessary.
45	118. It is suggested that factory should issue a procedure regarding security vetting of service contractors who require routine or scheduled access to the factory.
46	119. It is suggested that factory should send out corrective action notices to vendors or subcontractors in the event they do something to violate security policies or procedures.
47	127. It is suggested that factory should write down threat awareness program and publish it to all employees.
48	128. It is suggested that factory should provide additional security training to employees working in shipping and receiving areas.
49	130. It is suggested that the security training and threat awareness policies and procedures should be documented, periodically assessed to ensure compliance, and updated as necessary.

Auditor to Add Numbers as Necessary

Part 7 – Conclusion: In order for Unique to continue to do business with this manufacturer, the manufacturer must take steps to increase its security by answering "Yes" to more of the questions prior to the next Audit. Even if manufacturer passes the Audit, manufacturer must take steps to increase its score before the next Audit. The requirements for the manufacturer are as follows:

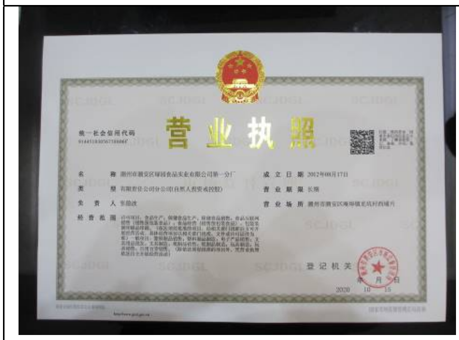
Audit Score	Requirement
85 – 130	Increase score by ten (10) points or more (if possible) before next Audit. Next Audit will take place in FIVE (5) years.
60 – 84	Increase score to eighty-five (85) or more (if possible) before next Audit. Next Audit will take place within three (3) year.

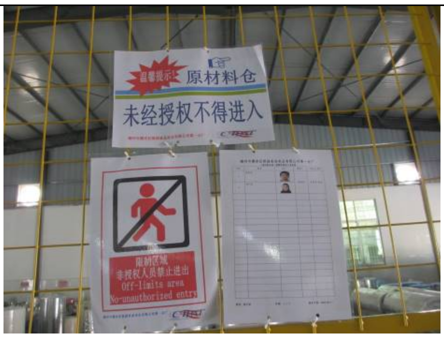
59 and Below	Increase score to sixty (60) or more before next Audit. Within sixty (60) days of the date you reply to this Report, Unique will perform a Follow-Up Audit at the Manufacturer's facility to confirm that the Manufacturer has performed the Corrective Action Plan as required.

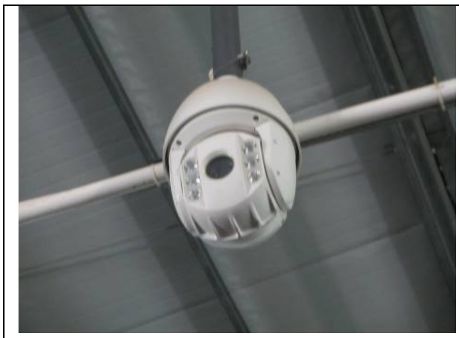
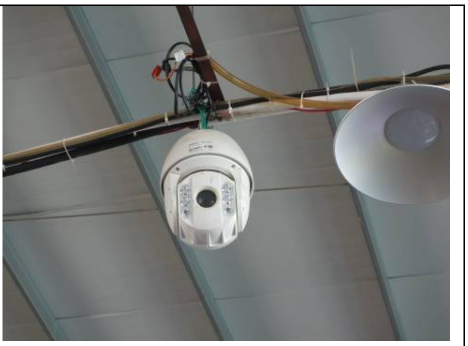
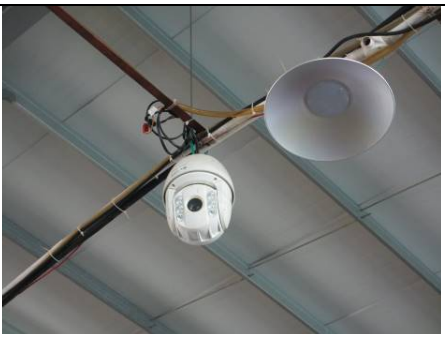
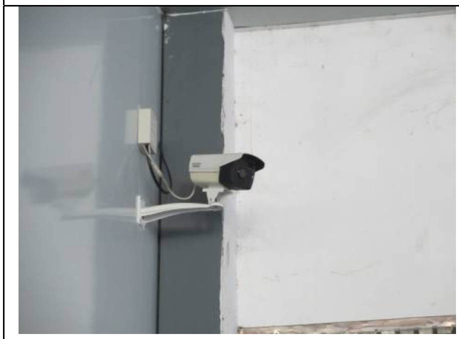
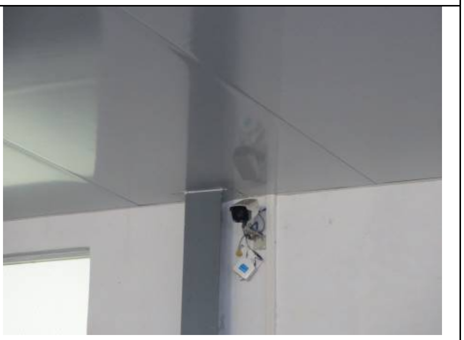
If the Manufacturer does not:
(a) respond within sixty (60) days with a written commitment to improve, and with proof of Corrective Action (where requested by Unique); and
(b) increase its score to sixty (60) or more before the next Audit;
then the Manufacturer will no longer be certified to do business with Unique, and Unique will stop placing new orders with the Manufacturer.

The Auditor signing below verifies that the information set forth in this form is correct. The Auditor is instructed to provide one copy of this report to the Manufacturer, and maintain the original for Unique's files.
Auditor on behalf of Unique Industries:

By:	Sam Luo
Name:	Sam Luo
Title:	Senior QA Specialist
Date of Report:	Nov 17 2020
Phone:	852-23428482
Fax:	852-23428485
E-Mail	sam.luo@ufefavors.com.cn/quality@favors.com.hk / martin.mak@favors.com.hk

Appendix:		
Photos attached:		
 营业执照 统一社会信用代码 名称 潮州市潮安区绿园食品实业有限公司第一分厂 类型 有限责任公司分公司(自然人投资或控股) 负责人 [illegible] 经营范围 [illegible] 成立日期 2012年09月17日 营业期限 长期 营业场所 潮州市潮安区[illegible] 登记机关 2020 年 10 月 15 日 Factory Business license 工厂营业执照	 潮州市潮安区绿园食品实业有限公司第一分厂 CHAOZHOU LUYUAN FOOD INDUSTRIAL CO.,LTD NO.1BRANCH FACTORY Factory name 工厂名称	 北纬 23°27 东经 116°39 2020.11.16 绿园食品实业有限公司龙坑分厂 Factory gate 工厂大门
 CCTV camera at factory gate 工厂大门闭路监控设备	 CCTV system at factory 工厂闭路监控系统	 Monitoring record at factory **工厂闭路监控记录**
 Factory wall 工厂围墙	 CCTV camera at factory Wall 工厂围墙闭路监控设备	 Raw material warehouse 原材料仓库

 CCTV camera at material warehouse 原材料仓库闭路监控设备	 温馨提示 原材料仓 未经授权不得进入 限制区域 非授权人员禁止进出 Off-limits area No unauthorized entry Notice for restricted area at raw material warehouse 原材料仓库限制区域标识	 复膜车间 Laminating workshop
 CCTV camera at Laminating workshop 复膜车间闭路监控设备	 Slaking workshop 熟化车间	 CCTV camera at slaking workshop 熟化车间闭路监控设备
 Cutting workshop 裁切车间	 CCTV camera at cutting workshop 裁切车间闭路监控设备	 Printing workshop 印刷车间

 CCTV camera at printing workshop 印刷车间闭路监控设备	 Bag making workshop 制袋车间	 CCTV camera at bag making workshop 制袋车间闭路监控设备
 Balloon hanging workshop 挂球车间	 CCTV camera at balloon hanging workshop 挂球车间闭路监控设备	 Punch Machinery workshop 冲床车间
 CCTV camera at Punch Machinery workshop 冲床车间闭路监控设备	 Assembly workshop 装配车间	 CCTV camera at assembly workshop 装配车间闭路监控设备

 Packaging workshop 包装车间	 CCTV camera at packaging workshop 包装车间闭路监控设备	包装区 未经授权不得进入 限制区域 非授权人员禁止进出 Off-limits area No-unauthorized entry Notice for restricted area at packaging workshop 包装车间限制区域标识
 Finished goods warehouse 成品仓库	 CCTV camera at finished goods warehouse 成品仓库闭路监控设备	未经授权不得进入 限制区域 非授权人员禁止进出 Off-limits area No-unauthorized entry Notice for restricted notice at finished goods warehouse 成品仓库限制区域标识
 Loading area 装卸货区	 CCTV Camera at loading area 装卸货区闭路监控设备	限制区域 非授权人员禁止进出 Off-limits area No-unauthorized entry Notice for restricted area at loading area 装卸货区限制区域标识

Floodlight at loading area

装卸货区照明灯

Security equipment (lighting + walkie talkie+ patrol the rod)

保安设备（手电筒/对讲机/巡逻棍）

Badge for visitors (for visit/delivery/loading/interview purpose)

访客证件(访客/送货/装柜/应聘)

Security guard

保安员

Security guards patrol point and record

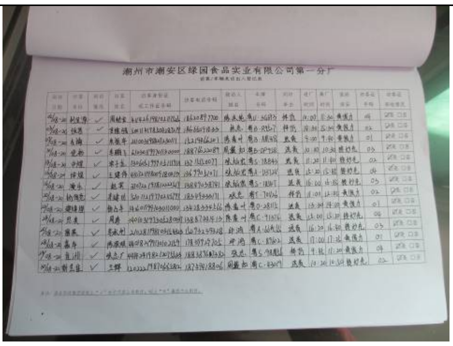
保安巡查点及记录

Parking area for visitor’s vehicle

访客车辆停车位

Parking area for factory’s vehicle

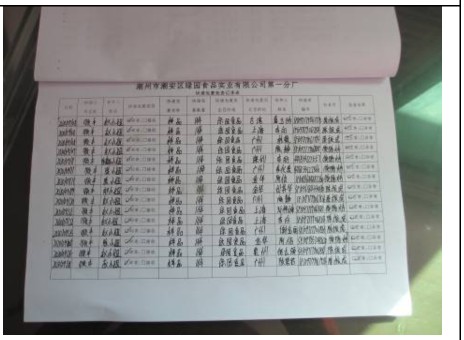
本厂车辆停车位



潮州市潮安区绿园食品实业有限公司第一分厂

Log book for visitors

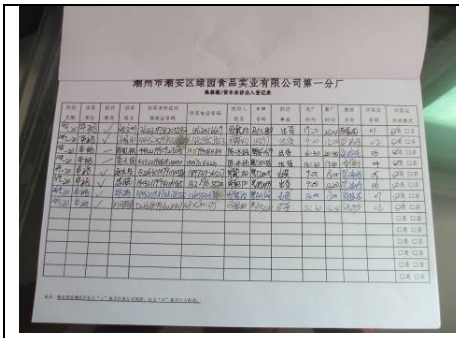
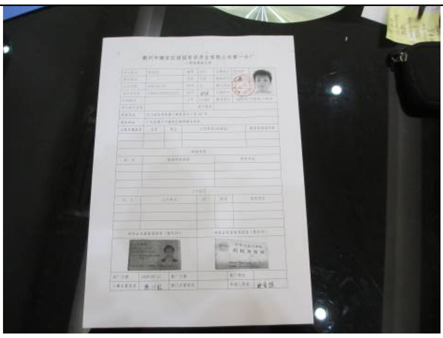
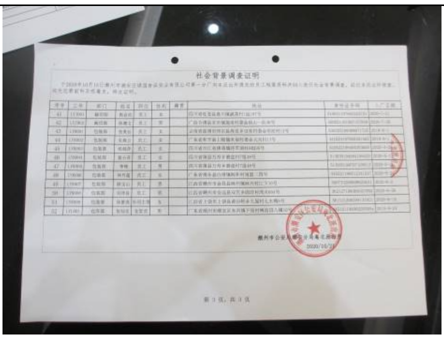
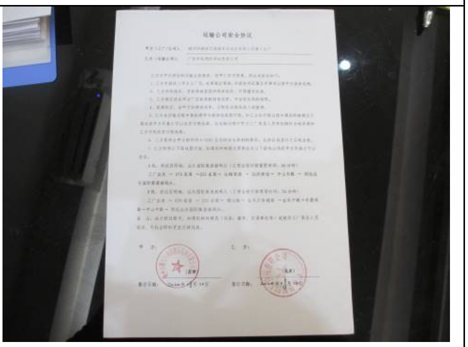
访客来访记录

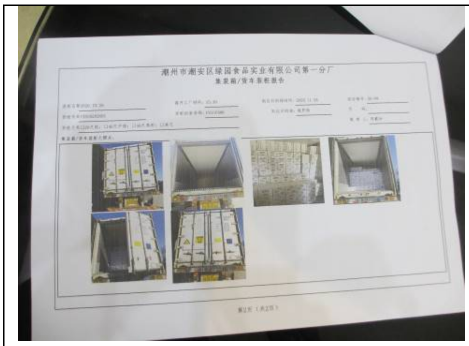
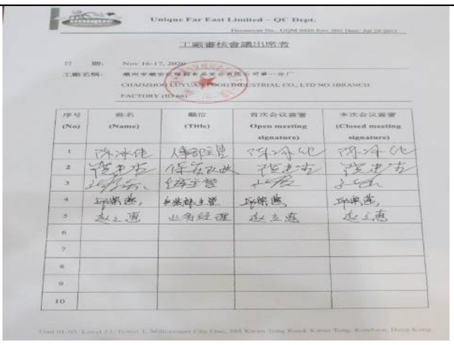


潮州市潮安区绿园食品实业有限公司第一分厂

Express delivery parcel inspection records

快递包裹安全检查记录

 Log book for containers/trailer 集装箱来访记录	 Personnel files 人事档案	 Staff card 员工厂证
 Fingerprint attendance checking system **指纹考勤系统**	 Background investigation proof record **背景调查证明**	 Suggestion box 意见箱
 Computer password protection 电脑密码保护	 Key box 钥匙箱	 Agreement with logistics agent 运输商协议书

 Photos of loading 集装箱/货车装柜照片 c	 Attendance record of C-TPAT audit 反恐审核出席人员签到表	

潮州市潮安区绿园食品实业有限公司第一分厂

集装箱/货车装柜报告

Unique Far East Limited – QC Dept.

工廠審核會議出席表

日 期: Nov 16-17, 2020

工廠名稱: 潮州市潮安区绿园食品实业有限公司第一分厂
CHAOZHOU LUYUAN FOOD INDUSTRIAL CO., LTD NO.1BRANCH FACTORY (ID:[illegible])

序号 (No)	姓名 (Name)	職位 (Title)	首次会议簽署 Open meeting signature)	末次会议簽署 (Closed meeting signature)
1	陈泳伟	人事部经理	陈泳伟	陈泳伟
2	[illegible]	保安队长	[illegible]	[illegible]
3	[illegible]	仓主管	[illegible]	[illegible]
4	邱[illegible]燕	品管部主管	邱[illegible]燕	邱[illegible]燕
5	赵立惠	业务经理	赵立惠	赵立惠
6				
7				
8				
9				
10				