TEST REPORT

Report No.:	BCTC2506327532-2EN1
Applicant:	SHENZHEN YUNJI INTELLIGENT TECHNOLOGY CO.,LTD
Product Name:	Smart Phone
Test Model:	WP55
Tested Date:	2025-06-20 to 2025-07-03
Issued Date:	2025-07-22

Shenzhen BCTC Testing Co., Ltd.

Product Name:	Smart Phone
Trademark:	OUKITEL
Model/Type reference:	WP55 WP35,WP35 Pro,WP39,WP39 Pro,WP55 Pro,WP55 Ultra, WP55 Plus,WP60,WP61 TI,WP61 Ultra
Prepared For:	SHENZHEN YUNJI INTELLIGENT TECHNOLOGY CO.,LTD
Address:	202, Building A2, Silicon Valley Power Intelligent Terminal Industrial Park, No. 20, Dafu Industrial Zone, Kukeng Community, Guanlan Street, Longhua District, Shenzhen,China
Manufacturer:	SHENZHEN YUNJI INTELLIGENT TECHNOLOGY CO.,LTD
Address:	202, Building A2, Silicon Valley Power Intelligent Terminal Industrial Park, No. 20, Dafu Industrial Zone, Kukeng Community, Guanlan Street, Longhua District, Shenzhen,China
Prepared By:	Shenzhen BCTC Testing Co., Ltd.
Address:	1-2/F., Building B, Pengzhou Industrial Park, No.158, Fuyuan 1st Road, Zhancheng, Fuhai Subdistrict, Bao'an District, Shenzhen, Guangdong, China
Sample Received Date:	2025-06-20
Sample tested Date:	2025-06-20 to 2025-07-03
Issue Date:	2025-07-22
Report No.:	BCTC2506327532-2EN1
Test Standards:	EN 18031-2:2024
Test Results:	PASS
Remark:	This is RED Common Security test report

Tested by:

Jason Luo

Jason Luo/ Project Handler

Approved by:

Zero Zhou/Reviewer

The test report is effective only with both signature and specialized stamp. This result(s) shown in this report refer only to the sample(s) tested. Without written approval of Shenzhen BCTC Testing Co., Ltd, this report can't be reproduced except in full. The tested sample(s) and the sample information are provided by the client.

Table Of Content

(Note: N/A Means Not Applicable)

1. Version

Report No.	Issue Date	Description	Approved
BCTC2506327532-2E	2025-07-17	Original	Invalid
BCTC2506327532-2EN1	2025-07-22	Revised	Valid
Note: Update series model.			

2. Test Summary

The Product has been tested according to the following specifications:

Mechanism	Requirement	Assessment	Verdict
ACM	ACM-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	ACM-2	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	ACM-3	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
	ACM-4	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
	ACM-5	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
	ACM-6	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
AUM	AUM-1-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	AUM-1-2	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	AUM-2-1	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	AUM-2-2	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
	AUM-3	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	AUM-4	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	AUM-5-1	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	AUM-5-2	Conceptual	Pass
		Functional completeness	N/A

		Functional sufficiency	Pass
	AUM-6	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
SUM	SUM-1	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	SUM-2	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	SUM-3	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
SSM	SSM-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	SSM-2	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	SSM-3	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
SCM	SCM-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	SCM-2	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	SCM-3	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	SCM-4	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
LGM	LGM-1	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	LGM-2	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	LGM-3	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
	LGM-4	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass

DLM	DLM-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
UNM	UNM-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	UNM-2	Conceptual	Pass
		Functional completeness	N/A
		Functional sufficiency	Pass
CCK	CCK-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	CCK-2	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	N/A
	CCK-3	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
GEC	GEC-1	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
	GEC-2	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	N/A
	GEC-3	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	N/A
	GEC-4	Conceptual	N/A
		Functional completeness	N/A
		Functional sufficiency	N/A
	GEC-5	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	N/A
	GEC-6	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass
	GEC-7	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	N/A
CRY	CRY-1	Conceptual	Pass
		Functional completeness	Pass
		Functional sufficiency	Pass

Note:
PASS indicates that test result meets the requirement.
FAIL indicates that test result does not meet the requirement.
N/A indicates that Not Applicable.

3. Product Information

3.1 Product Information

Model/Type reference:	WP55,WP35,WP35 Pro,WP39,WP39 Pro,WP55 Pro,WP55 Ultra, WP55 Plus,WP60,WP61 TI,WP61 Ultra
Model differences:	All the model are the same circuit and RF module, except model names and appearance of the color. The color of the tested sample is black.The tested model is WP55.
Interface of Internet connected:	Bluetooth, WIFI, LTE
Firmware Version:	Android 15
Software Version:	OUKITEL_WP55_EEA_V18_20250612
Hardware Version:	N/A
MCU:	MT6855
APP(Android):	N/A
APP(iOS):	N/A

4. Test Facility And Test Instrument Used

4.1 Test Facility

All measurement facilities used to collect the measurement data are located at Shenzhen BCTC Testing Co., Ltd. Address: 1-2/F., Building B, Pengzhou Industrial Park, No.158, Fuyuan 1st Road, Zhancheng, Fuhai Subdistrict, Bao'an District, Shenzhen, Guangdong, China.

4.2 Test Instrument Used

Equipment	Equipment No.	Manufacturer	Model
Computer Server	BCTC-EMC-342	Dell	R750XS
Computer Server	BCTC-EMC-343	Dell	R750XS
Computer Storage	BCTC-EMC-344	Dell	ME5024
Computer	BCTC-EMC-317	Dell	OptiPlex Tower Plus 7020 XCTO

Software	Software No.	Manufacturer	Version
Nessus Pro	BCTC-EMC-S018	Tenable	V10.8.4
Nmap	BCTC-EMC-S016	Insecure	V7.95

5. Requirements and Assessments

Clause	Requirements	Assessments
6.1.1	**[ACM-1] Applicability of access control mechanisms** The equipment shall use access control mechanisms to manage entities' access to security assets and network assets, except for access to security assets or network assets where: — public accessibility is the equipment's intended functionality; or — physical or logical measures in the equipment's targeted operational environment limit their accessibility to authorized entities; or — legal implications do not allow for access control mechanisms.	Pass
6.1.2	**[ACM-2] Appropriate access control mechanisms** Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets.	Pass
6.1.3	**[ACM-3] Default access control for children in toys** If the equipment is a toy, for each privacy function where children can access external content and children's access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall by default ensure that children's access to external content via the privacy function is restricted to content from authorized entities.	N/A
6.1.4	**[ACM-4] Default access control to children's privacy assets for toys and childcare Equipment** If the equipment is a toy or childcare equipment, any children's privacy function and personal information access control mechanisms required per ACM-1 shall by default restrict, apart from the child's or their parental/guardians, any third-party access to the children's privacy function and personal information processed by the equipment, except for authorised accesses which are required for the equipment's intended functionality.	N/A
6.1.5	**[ACM-5] Parental/Guardian access controls for children in toys** If the equipment is a toy, for each security and privacy asset that is accessible by children, any access control mechanism required per	N/A

	ACM-1 managing the children's access, shall be configurable by an authorized entity to restrict children's access to the protected security and privacy assets.	
6.1.6	**[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys** If the equipment is a toy, for each children's privacy asset that is accessible by entities, other than the children or their parents or guardians, and where those other entities' access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall be configurable by an authorized entity to restrict the other entities' access to the managed children's privacy assets.	N/A
6.2.1.1	**[AUM-1] Applicability of authentication mechanisms** **[AUM-1-1] Requirement network interface** Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to: — read confidential network function configuration or confidential security parameters; or — modify sensitive network function configuration or sensitive security parameters; or — use network functions or security functions, except for access: — to network functions or network function configuration where the absence of authentication is required for the equipment's intended functionality; or — via networks where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorised entities.	Pass
6.2.1.2	**[AUM-1] Applicability of authentication mechanisms** **[AUM-1-2] Requirement user interface** Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to: — read confidential network function configuration or confidential security parameters; or — modify sensitive network function configuration or sensitive security parameters; or — use network functions or security functions,	Pass

	except for access: — where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorized entities; and except for read only access to network functions or network functions configuration where access without authentication is needed: — to enable the intended equipment functionality; or — because legal implications do not allow for authentication mechanisms.	
6.2.2.1	**[AUM-2] Appropriate authentication mechanisms** **[AUM-2-1] Requirement one factor authentication** Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity's claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication).	Pass
6.2.2.2	**[AUM-2] Appropriate authentication mechanisms** **[AUM-2-2] Requirement two factor authentication** If the primary equipment's intended functionality is specifically processing personal information of special categories, for each access to personal information of special categories via user interfaces over network interface the authentication mechanisms shall support the verification of an entity's claim based on evidence derived from at least two different elements of the categories knowledge, possession and inherence (two factor authentication).	N/A
6.2.3	**[AUM-3] Authenticator validation** Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.	Pass
6.2.4	**[AUM-4] Changing authenticators** Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.	Pass
6.2.5.1	**[AUM-5] Password strength** **[AUM-5-1] Requirement for factory default passwords** If factory default passwords are used by an	Pass

	authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall: — be unique per equipment; and — follow best practice concerning strength; or — be enforced to be changed by the user before or on first use. NOTE The user can choose to not use any password.	
6.2.5.2	**[AUM-5] Password strength** **[AUM-5-2] Requirement for non-factory default passwords** If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: — be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or — be defined by an authorized entity within a network where access is limited to authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities. NOTE The user can choose to not use any password.	Pass
6.2.6	**[AUM-6] Brute force protection** Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks.	Pass
6.3.1	**[SUM-1] Applicability of update mechanisms** The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets, except for software: — where functional safety implications do not allow updatability; or — which is immutable; or — where alternative measures protect the affected security assets and/or network assets during the entire lifecycle of the equipment.	Pass
6.3.2	**[SUM-2] Secure updates** Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	Pass
6.3.3	**[SUM-3] Automated updates** Each update mechanism that is required per SUM-1 shall be capable of updating the software: — without human intervention at the	Pass

	equipment; or — via scheduling the installation of an update under human approval; or — via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment.	
6.4.1	**[SSM-1] Applicability of secure storage mechanisms** The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets where: — the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities.	Pass
6.4.2	**[SSM-2] Appropriate integrity protection for secure storage mechanisms** Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently.	Pass
6.4.3	**[SSM-3] Appropriate confidentiality protection for secure storage mechanisms** Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently.	Pass
6.5.1	**[SCM-1] Applicability of secure communication mechanisms** The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces, except for: — communicating security assets or network assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that network assets or security assets are not exposed to unauthorised entities; or — communicating security assets or network assets whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation.	Pass
6.5.2	**[SCM-2] Appropriate integrity and authenticity protection for secure communication Mechanisms** Each secure communication mechanism that is required per SCM-1 shall apply best	Pass

	practices to protect the integrity and authenticity of the security assets and network assets communicated, except for communicating security assets or network assets where: — a deviation from best practice for integrity or authenticity protection is required for interoperability reasons.	
6.5.3	**[SCM-3] Appropriate confidentiality protection for secure communication mechanisms** Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed, except for communicating security assets or network assets where: — a deviation from best practice for protecting confidentiality is required for interoperability reasons.	Pass
6.5.4	**[SCM-4] Appropriate replay protection for secure communication mechanisms** Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks, except for communicating security assets or network assets where: — a duplicate transfer does not impose a threat of a replay attack; or — a deviation from best practice for replay protection is required for interoperability reasons.	Pass
6.6.1	**[LGM-1] Applicability of logging mechanisms** The equipment shall use logging mechanisms for internal activities that are relevant to privacy assets and their protection (referred to as events), except for: — internal activities where a legal obligation prohibits logging.	Pass
6.6.2	**[LGM-2] Persistent storage of log data** Logging mechanisms that are required per LGM-1 shall store log data for related events in the equipment's persistent storage, except for events where: — related log data is stored outside the equipment.	Pass
6.6.3	**[LGM-3] Minimum number of persistently stored events** All log data stored in equipment's persistent storage by logging mechanisms that are required per LGM-1 shall always include: — a minimum number of the latest events;	Pass

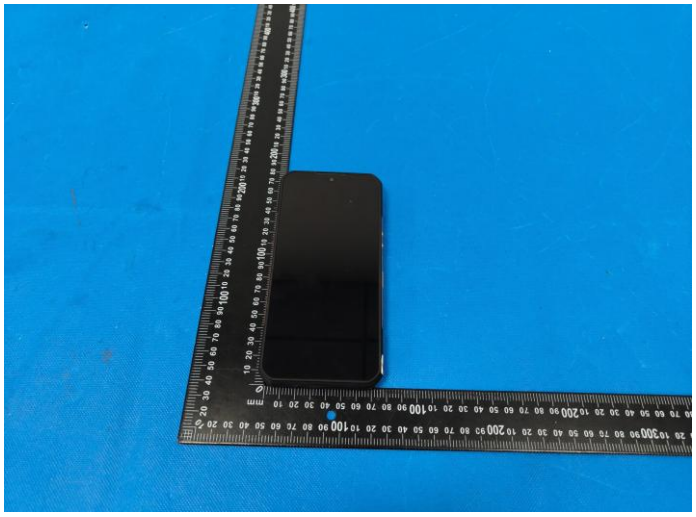
	and — the latest event.	
6.6.4	**[LGM-4] Time-related information of persistently stored log data** All log data stored in equipment's persistent storage by logging mechanisms that are required per LGM-1 shall include: — a timestamp if real time is available on the equipment; and — time-related information if real time is not available on the equipment.	Pass
6.7.1	**[DLM-1] Applicability of deletion mechanisms** The equipment shall provide a deletion mechanism that allows a user to delete their personal data and sensitive security parameters stored on the equipment.	Pass
6.8.1	**[UNM-1] Applicability of user notification mechanisms** The equipment shall provide user notification mechanism(s) for informing the user of the equipment about changes affecting the protection or privacy of personal information, except for changes where: — other methods of informing the user exist, which do not involve the equipment.	Pass
6.8.2	**[UNM-2] Appropriate user notification content** The content of a notification provided by a user notification mechanism that is required per UNM-1 shall include at least: — a description of a change; and — a description of how a change will affect the protection and privacy of personal information.	Pass
6.9.1	**[CCK-1] Appropriate CCKs** Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits, except for: — CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.	Pass
6.9.2	**[CCK-2] CCK generation mechanisms** The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for: — the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.	Pass
6.9.3	**[CCK-3] Preventing static default values for**	Pass

	preinstalled CCKs Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for: — CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or — CCKS key are shared parameters required for the equipment's intended functionality. NOTE Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.	
6.10.1	**[GEC-1] Up-to-date software and hardware with no publicly known exploitable Vulnerabilities** The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets, except for vulnerabilities: — that cannot be exploited in the specific conditions of the equipment; or — that have been mitigated to an acceptable residual risk; or — that have been accepted on a risk basis.	N/A
6.10.2	**[GEC-2] Limit exposure of services via related network interfaces** In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment.	Pass
6.10.3	**[GEC-3] Configuration of optional services and the related exposed network interfaces** Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service.	Pass
6.10.4	**[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces** The equipment's user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces,	N/A

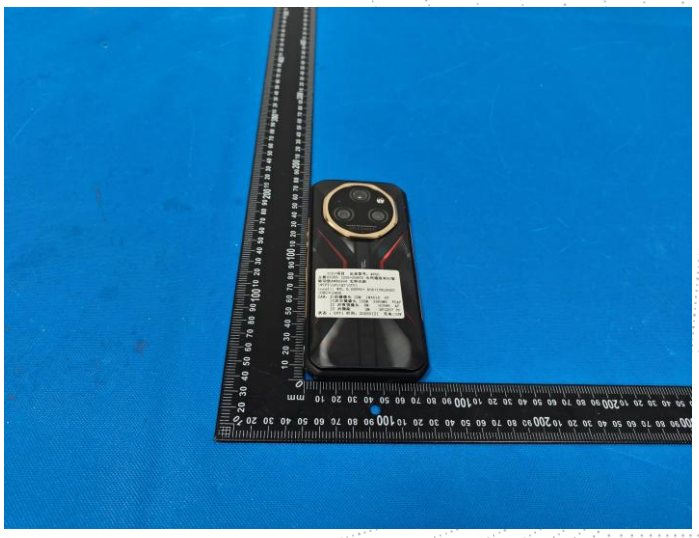
	which are delivered as part of the factory default state.	
6.10.5	**[GEC-5] No unnecessary external interfaces** The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.	Pass
6.10.6	**[GEC-6] Input validation** The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets.	Pass
6.10.7	**[GEC-7] Documentation of external sensing capabilities** All external sensing capabilities of the equipment that are related to the user's or subscriber's privacy shall be documented for the user.	Pass
6.11.1	**[CRY-1] Best practice cryptography** The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets, except for: — cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.	Pass

6. EUT Photographs

EUT Photo 1



EUT Photo 2



STATEMENT

1. The equipment lists are traceable to the national reference standards.

2. The test report can not be partially copied unless prior written approval is issued from our lab.

3. The test report is invalid without the "special seal for inspection and testing".

4. The test report is invalid without the signature of the approver.

5. The test process and test result is only related to the Unit Under Test.

6. Sample information is provided by the client and the laboratory is not responsible for its authenticity.

7. The quality system of our laboratory is in accordance with ISO/IEC17025.

8. If there is any objection to this test report, the client should inform issuing laboratory within 15 days from the date of receiving test report.

Address:
1-2/F., Building B, Pengzhou Industrial Park, No.158, Fuyuan 1st Road, Zhancheng, Fuhai Subdistrict, Bao'an District, Shenzhen, Guangdong, China

TEL: 400-788-9558

P.C.: 518103

FAX: 0755-33229357

Website: http://www.chnbctc.com

Consultation E-mail: bctc@bctc-lab.com.cn

Complaint/Advice E-mail: advice@bctc-lab.com.cn

※※※※※ END ※※※※※