



5<sup>th</sup> July 2017

**Mr Jody Cloutier**  
**Microsoft Corporation**  
**One Microsoft Way**  
**Redmond WA 98052-6399**  
**USA**

Dear Sir,

**SUBMISSION OF ANNUAL AUDIT REPORT FOR NETRUST CA - MICROSOFT WINDOWS CERTIFICATION AUTHORITY AGREEMENT**

We are pleased to enclose the following documents as part of the requirements stated in the Microsoft Windows Certification Authority Agreement:

1. Grant of Accredited CA status to Netrust, by the Controller of CA in Singapore, valid for period till 13 June 2019.
2. CA Audit Report of Netrust Certificate Authority dated 31<sup>st</sup> May 2017.
3. Print-out from the Infocomm Media Development Authority of Singapore's (IMDA) website on the current accreditation status of Netrust.

In addition, please note that Netrust's existing CA, Netrust CA1, has been in existence since 30th March 2001. It has a lifespan of 20 years till 30th March 2021. We would like to officially notify Microsoft that Netrust has setup a new Root CA (Netrust CA 2), with two subordinate CAs (Netrust CA 2-1 and Netrust CA 2-2), and these are included in the recent audit and accreditation by the Controller of CA, Singapore. The root certificates of the Netrust CA 2 and the Subordinate CAs are available for download at: <https://www.netrust.net/root-cert>. The certificates have thumbprints as indicated below:

**Root CA**

**Netrust CA 2 Root Certificate Thumbprint:**

0a b5 c3 cd 74 48 b8 6d 71 1e 77 a5 49 83 8b 87 ce 52 5f 7f

**Subordinate CAs**

**Netrust CA 2-1 Certificate Thumbprint:**

11 1a a9 d4 d2 e9 e3 77 8c ff 71 86 5c f8 bb e8 1c df 42 a8

**Netrust CA 2-2 Certificate Thumbprint:**

a9 6e d0 93 d6 26 78 cc f0 18 97 94 0e 0e 04 5b 4c e9 0b 28

We would need to incorporate the new Root Certificates into the Microsoft Root Store as well. Please contact me at telephone: +65-6212-1368 or email: [jongai.foo@netrust.net](mailto:jongai.foo@netrust.net) should you require any clarifications on the documents submitted.

Yours Sincerely,

---

**FOO JONG AI**  
**Chief Executive Officer**

# Grant of Accreditation of Certification Authority

Pursuant to regulation 3 of the Electronic Transactions (Certification Authority) Regulations 2010, the Controller hereby grants accreditation to the following Company as an accredited certification authority:

Name of Company: Netrust Pte Ltd  
Address: 70 Bendemeer Road  
#05-03 Luzerne  
Singapore 339940  
Date of Accreditation: 14 June 2017  
Valid Up To: 13 June 2019  
Accreditation No.: CAA000001



Controller of Certification Authority

# CERTIFICATION AUTHORITY AUDIT REPORT

**NETRUST PTE LTD**

**Ref: Q2017/WLB/12336**

31<sup>st</sup> May 2017

Version 1.0 (Final)



**Prepared by:**  
Elean Kwek,  
Associate Security Consultant  
Professional Security Services

**Reviewed by:**  
Edwina Tan,  
Project Manager,  
Senior Security Consultant  
Professional Security Services

## COPYRIGHT NOTICE

This document is QUANN Asia Pacific report to **Netrust Pte Ltd** and shall be used strictly for such purpose only. All information in this document must be kept strictly confidential and should only be disclosed to AUTHORIZE employees of **Netrust Pte Ltd**. This document should not be circulated to any third party without the prior written approval from **Netrust Pte Ltd** and QUANN Asia Pacific



**QUANN Asia Pacific Pte Ltd**  
**23 Serangoon North Ave 5**  
**#06-01 BTH Centre**  
**Singapore 554530**

**To: Netrust Pte Ltd**

**SIGNOFF & ACKNOWLEDGMENT**

QUANN Asia Pacific would like to take this opportunity to thank the Management and staff of **Netrust Pte Ltd** for all their assistance and time during the course of this assessment & review.

This report is intended solely for use by the Management of **Netrust Pte Ltd** and QUANN Asia Pacific accept no responsibility for any reliance on the report by any third parties, unless our permission is sought for the provision of the particular report to specified third parties and such request is given to us in writing prior to provision of the report.

This acknowledgement represents the agreement between QUANN Asia Pacific and **Netrust Pte Ltd** with respect to the objectives, obligations and responsibilities performed in the Certification Authority Audit had been completed.

The results of the Certification Authority Audit – vulnerabilities identified along with recommendations are documented in this report. The recommendations provided by QUANN Asia Pacific are to assist **Netrust Pte Ltd** in strengthening the security posture of their network. It is necessary to ensure that the vulnerabilities identified are resolved promptly to minimize threats.

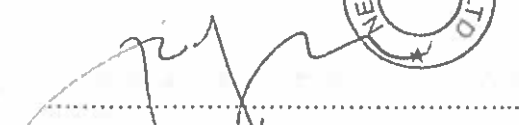
The information contained in this document represents the view of QUANN Asia Pacific on the vulnerabilities as of the date of the assessment. QUANN Asia Pacific shall not be held liable for any damaged due to the negligence of the vulnerabilities.

**CERTIFICATION AUTHORITY  
AUDIT REPORT**

**NETRUST PTE LTD**  
**Ref: Q2017/WLB/12336**

**Version 1.0 (Final)**

Accepted by:

  
Date: 14/06/2017



Prepared by:

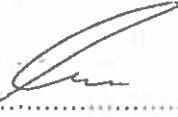
Elean Kwek  
*Associate Security Consultant*



Date: 12/06/2017

Reviewed by:

Edwina Tan  
*Project Manager, Senior Security Consultant*



Date: 14/06/2017



Please return or fax this copy to QUANN Asia Pacific at +65 6788 8883

## Reports, Copyright and other intellectual Property Rights

Except to the extent expressly set out otherwise in the agreement between QUANN and the Customer for this project ("Agreement"):

(a) This report and any information, advice, recommendations or content of any other reports, presentations or other communications that QUANN provides under the Agreement (each, a "Report") are for the Customer's internal use only, and for the avoidance of doubt, copies of the Report are permitted to be made by the Customer for its internal use only. The Report constitutes confidential information. The Customer shall not disclose the Report (or any portion or summary of a Report) externally unless with QUANN's express prior written consent. QUANN shall be entitled to stipulate terms before consenting to any external parties' proposed access to the Report, and further the Customer shall inform such external parties that they may not rely on it for any purpose unless with QUANN's prior written consent;

(b) Any copyright and other intellectual property rights resulting from the performance of the Agreement that is conceived, developed, discovered or reduced to practice by QUANN, including without limitation any QUANN's original programs, specifications, reports or other items arising in the course of or resulting from the project (collectively, "QUANN Foreground IPR"), shall be the exclusive property of QUANN;

(c) QUANN hereby grants to the Customer a non-transferable and non-exclusive license to use the Report and QUANN Foreground IPR contained therein provided always that it shall not be used in any way that is detrimental to QUANN's interests;

Notwithstanding any provision to the contrary, nothing shall affect any of QUANN's or the Customer's or any third party's ownership of intellectual property rights which are created prior to or independently of the Agreement ("Background IPR"). The Customer remains the sole owner of all intellectual property rights and knowhow which are owned by the Customer ("Customer's Background IPR"), and the Customer has granted to QUANN the relevant licenses and rights to such Customer's Background IPR to such extent which has enabled QUANN to carry out the works under the Agreement. QUANN remains the sole owner of all intellectual property rights and knowhow which are owned by QUANN ("QUANN Background IPR") and used in connection with the works carried out herein, except to the extent that intellectual property rights associated with equipment or software not created by QUANN ("Third Party Background IPR") shall continue to belong to the relevant intellectual property rights owners.

## Confidential Information

The Report constitutes confidential information. The Customer shall use confidential information for the purposes of the Agreement only, and treat and safeguard (and ensure that its employees, directors, officers and representatives treat and safeguard) the Report as confidential information. Insecure communications mediums should not be used to distribute the Report. All copies and backups of the Report should be maintained on protected storage at all times. Information contained within the Report shall not be shared with anyone unless the recipient(s) are authorised to view the information.

## Limitations and Disclaimers

The Report and/or any other vulnerability results cannot and do not guarantee security and regulatory compliance. It is the sole responsibility of the Customer to maintain the security of the Customer's systems in continuous efforts against emerging threats and the Customer's compliance to its regulatory, statutory and legal obligations, and the Customer remains solely responsible and accountable for these tasks. QUANN does not assume any responsibilities nor make any warranty or claim of any kind, whatsoever, about the accuracy, usefulness or completeness of any information in the Report. By using such information, the Customer shall be deemed to agree to indemnify and hold harmless QUANN from any loss, damage or liability whatsoever incurred by the Customer in connection with such use.

QUANN may use various software, designs, utilities, tools, models, systems and other methodologies and know-how (collectively, "Materials") owned by or licensed to QUANN to carry out the works under the Agreement. For the avoidance of doubt, the works carried out are subject to the terms and conditions (including without limitation any restrictions therein) of the license agreements regarding the Materials.

Further, except to the extent expressly set out otherwise in the Agreement and to the maximum extent permitted by law, all other warranties (implied or otherwise), including without limitation any warranty of merchantability or fitness for a particular purpose, are excluded by QUANN.

NOTWITHSTANDING ANY PROVISION TO THE CONTRARY, THE WORKS UNDER THE AGREEMENT ARE NOT A GUARANTEE AGAINST MALICIOUS CODE, DELETERIOUS ROUTINES AND OTHER TECHNIQUES AND TOOLS EMPLOYED BY COMPUTER HACKERS AND OTHER THIRD PARTIES TO CREATE SECURITY EXPOSURES WHETHER IN REGARD TO A PHYSICAL ENVIRONMENT OR CYBER ENVIRONMENT (AND WHETHER MALICIOUS OR OTHERWISE). QUANN MAKES NO WARRANTY, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND/OR VULNERABILITIES (WHETHER IN REGARD TO A PHYSICAL ENVIRONMENT, CYBER ENVIRONMENT OR OTHERWISE) WILL BE DETECTED OR THAT THE WORKS UNDER THE AGREEMENT WILL RENDER THE CUSTOMER'S (OR ANY OTHER END-USER'S) PREMISES, ASSETS, EQUIPMENT, NETWORK, COMPUTER SYSTEMS, SOFTWARE AND/OR APPLICATIONS SAFE FROM INTRUSIONS AND OTHER SECURITY BREACHES.

The following apply where Assessment Services are provided, and "Assessment Services" means security penetration testing services or other invasive security services or anything analogous or substantially similar to the foregoing:

- (a) Certain laws and regulations prohibit the unauthorized penetration of computer networks and systems. If Customer engaged QUANN to perform Assessment Services pursuant to the Agreement, Customer acknowledges and agrees that such engagement constituted permitted access to Customer's networks and computer systems;
- (b) In the event that one or more of the IP Addresses identified by Customer are associated with computer systems owned, managed, and/or hosted by a third party service provider ("Host") or if any third party consents are so required for any other reason, Customer has procured the consent and authorization from such Host(s) or third parties necessary for QUANN to perform the works under the Agreement, including where requested, the Assessment Services;
- (c) Notwithstanding any provision to the contrary, QUANN shall assume no responsibility for any claims, liability, loss or damages whether directly or indirectly as a result of the Assessment Services (which would include the conduct of penetration tests) under any circumstances, except where due to the wilful default and gross negligence of QUANN.

#### Out-of-Scope

Notwithstanding any provision to the contrary, QUANN shall not be liable for any claims, demands, actions, judgments, damages, losses, costs or expenses whatsoever (whether resulting directly or indirectly) and howsoever arising from, caused by or in connection with the performance by QUANN of any service which QUANN is not obliged to provide under the Agreement, but at the request of the Customer undertook to perform.

## 1. Executive Summary

The objective of this assessment is to detect any vulnerability in **Netrust Pte Ltd's** IT assets under the scope and to check the effectiveness of the implemented security controls in preventing any potential unauthorized information access through the aforementioned IT assets. The list of in-scope assessments can be found in Section 4 of this document.

### a. Certification Authority Audit

The objective of this assessment on **Netrust Pte Ltd** was to review whether **Certification Authority** process is developed accordance to Security Guidelines for Certification Authorities Version 2.0 policies. Furthermore, it shall also evaluate the security controls implemented in the application.

Except for the findings mentioned in Section 5, **Netrust** was in all material respects, in compliance with the Security Guidelines for Certification Authorities Version 2.0 policies. **QUANN** has provided recommendations under Section 5 to address the issues identified during the review.

Below is the summary of findings for this engagement. Detailed observations and our recommendations to mitigate the risks can be found in Section 5 of this document.

| Severity level | Findings | Areas of Findings  |
|----------------|----------|--|
| High           | -        | -  |
| Medium         | 1        | 5.1 Physical and Environmental Controls Lapse                    |
| Low            | 3        | 5.2 Record Management Lapse – Records of Periodic Review Absent  |
|                |          | 5.3 Documentation Management Lapse                               |
|                |          | 5.4 Vulnerability Management Lapse – Periodic Assessment Not Met |
| <b>Total</b>   | <b>4</b> |  |

*Chart 1: Number of Vulnerabilities by Severity Level*

We are of the opinion that even when all the above vulnerabilities have eventually been addressed – in order to maintain on-going security posture of the network infrastructure, **Netrust Pte Ltd** should consider the following:

- ⇒ To conduct periodic IT Security Assessment as well as Security Audit reviews especially when after major changes in the systems and infrastructure.



## TABLE OF CONTENT

---

|   |    |
|---|----|
| 1. Executive Summary.....   | 6  |
| 2. Introduction.....  | 8  |
| 3. Risk Classification.....   | 11 |
| 4. Test Scope.....  | 15 |
| 5. Certification Authority Audit.....                                     | 16 |
| 5.1 Physical and Environmental Controls Lapse (M).....                    | 16 |
| 5.2 Record Management Lapse – Records of Periodic Review Absent (L).....  | 18 |
| 5.3 Documentation Management Lapse (L).....                               | 19 |
| 5.4 Vulnerability Management Lapse – Periodic Assessment Not Met (L)..... | 20 |
| 6. Version Control.....   | 21 |

## 2. Introduction

Netrust was established in May 1997 as the first Certification Authority ("CA") in Southeast Asia. Netrust provides individuals, businesses and government organizations with a complete online identification and security infrastructure to enable secure electronic transactions via the Internet and other wireless media.

In its capacity as a CA, Netrust acts as a trusted third party ("TTP") that issues and manages digital certificates. Netrust maintains a Public Key Infrastructure ("PKI") certification service and in its CA role creates and signs X.509 digital certificates which bind individuals, organizations and application servers with the particular public key of each subscriber.

Netrust's PKI provides a secure environment where faceless electronic transactions can take place with trust on the Internet, Intranet and on wireless networks. It issues to participants of this environment, digital certificates - which are equivalent to electronic IDs - that give online identities to individuals, organizations and application servers. Netrust's digital certificates can be issued globally and provide complete online identification and security for secure electronic transactions.

Netrust issues a range of digital certificates for online applications including secure access to government applications, Internet banking, supply chain management, virtual private networks and secure access to intranet portals. It supports the core Security Guidelines of Authentication, Authorization, Confidentiality, Data Integrity and Non-Repudiation.

The Electronic Transactions Act ("ETA") was first enacted on 10 July 1998 to create a legal framework for electronic commerce transactions in Singapore. Following the ETA, the Electronic Transactions (Certification Authority) Regulations ("ETR") came into operation on 10 February 1999 to provide regulations for the licensing and regulation of certification authorities ("CAs") in Singapore. The ETA 1998 has since been replaced by the Electronic Transactions Act 2010. The Controller of Certification Authorities ("CCA") also published security guidelines in 2010 to establish the security criteria for the management, systems and operations of CAs. The voluntary licensing programme aims to promote high integrity licensed CAs that can be trusted. The CCA awarded the CA License to Netrust in June 2001.

Netrust CA1 would reach its lifespan by March 2021. In preparation for the migration, Netrust has setup a new Root CA2, with two Subordinate CAs, CA2-1 & CA2-2.

The ETR requires regular audits to be conducted on Netrust to provide assurance that the IT systems and processes of Netrust fulfill the requisite Security Guidelines, as set forth in the security guidelines issued by the CCA.

Netrust Pte Ltd ("Netrust") has engaged QUANN Asia Pacific to perform a Certificate Authority Audit from 10<sup>th</sup> April 2017 to 13<sup>th</sup> April 2017 on their IT assets, CA1, CA2 (CA2-1 & CA2-2).

#### 1. Certification Authority Audit

- Assessment Period: 10<sup>th</sup> April 2017 – 13<sup>th</sup> April 2017
- Audit Criteria:
  - Security Guidelines for Certification Authorities Version 2.0

Note: This document was issued by the Controller of Certification Authority from the Info-communications Media Development Authority ("IMDA") of Singapore

- Audit Scope:
  - Certification Authority Overall Governance
    1. Obligations to Subscribers, Relying Party and User Community
    2. Certificate Practice Statement (CPS) and Certificate Policies (CP)
    3. Security Management
    4. Risk Management
    5. Personnel Controls
    6. Subscribers' Data
    7. Incident Management
    8. Business Continuity Planning
  - Certificate Management Controls
    1. Registration Process
    2. Generation Process
    3. Issuance Process
    4. Publication Process
    5. Renewal Process
    6. Certificate Suspension Process
    7. Revocation Process
    8. Archival Process
    9. Audit Trails
  - Key Management Controls
    1. Generation
    2. Distribution
    3. Storage
    4. Usage
    5. Backups
    6. Key Change
    7. Destruction
    8. Key Compromise
    9. Key Archival
    10. Cryptographic Engineering
  - System and Operational Controls
    1. Physical Security
    2. General Security Controls
    3. General Operational Controls
    4. Change and Configuration Management
    5. Network Security
    6. Monitoring and Audit Trails
  - Application Integration Controls

The overall testing procedure consisted of:

- Compliance verification
- Compiling the results of all analysis into report.

The report here is presented in the following format:

- Summary of vulnerabilities identified.
- Overview of area tested and tests performed.
- Detailed explanation of vulnerabilities found with recommended fixes.

The limitations of the Certificate Authority Audit are as follows:

- **Use of Our Report**

This report has been prepared solely for the management of Netrust. We would not generally permit the use of our deliverables, or references to it, in material disseminated to the general public or third parties without our written permission, with the exception of the Info-communications Media Development of Singapore ("IMDA").

- **Limitation of Controls**

Control policies and procedures designed to address specified control objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected. Therefore, constant monitoring is needed to ensure that system controls that exist remain effective over time.

- **Limitation of Liability**

Netrust will indemnify and hold harmless QUANN Asia Pacific from claims, liabilities and costs to third parties where Netrust divulges any advice rendered by QUANN Asia Pacific pursuant to this engagement without QUANN Asia Pacific's consent to such parties and such third parties claim against QUANN Asia Pacific for losses suffered by them as a result of their reliance on such advice.

### 3. Risk Classification

#### 3.1 Impact Rating

An analysis of impact of the findings was performed based on the confidentiality, integrity and availability impact, wherever applicable. The impact ratings are as follows:

| Impact Rating  | Description of rating  |
|--|--|
| <p style="text-align: center;"><b>High (H)</b></p>   | <p>When impact of vulnerability poses an <i>immediate</i> or <i>direct</i> effect resulting either loss of confidentiality, integrity and availability of the information asset of the organization.</p> <p>Example:</p> <ol style="list-style-type: none"> <li>1) Reliable exploitation of code that result in compromise of system.</li> <li>2) Processes that involved information assets without procedures in place.</li> </ol>   |
| <p style="text-align: center;"><b>Medium (M)</b></p> | <p>When impact of vulnerability is not immediately exploitable but has a potential of deteriorating to higher impact level resulting high impact as outlined above.</p> <p>Example:</p> <ol style="list-style-type: none"> <li>1) Unreliable exploitation of code that result in system instability such as denial of service</li> <li>2) Processes that involved information assets with procedures in place but not maintained to company standard such as frequent record inconsistency.</li> </ol>   |
| <p style="text-align: center;"><b>Low (L)</b></p>    | <p>When impact of vulnerability has a remote chance of further deteriorating to the above Medium impact level OR when it provides excessive information that may lead to compromising confidentiality, integrity, and/or availability of the information assets.</p> <p>Example:</p> <ol style="list-style-type: none"> <li>1) Information leakage gathered during service probing.</li> <li>2) Processes that involved information assets with procedures in place but not maintained to company standard such as slight record inconsistency.</li> </ol> |

*Table 1: Impact Rating Matrix*

### 3.2 Likelihood Rating

The threat likelihood is estimated and determined based on detailing aspects of the threat agent, and the amount of expertise needed by the threat agent to perform the system compromise. The likelihood ratings are as follows:

| Likelihood Rating | Description of rating   |
|-------------------|---|
| High (H)          | <p>When likelihood of vulnerability occurrence is of high frequency OR ease of vulnerability exploitation by unskilled attackers.</p> <p>Example:<br/>1) 'Point and click' exploits available for unskilled attackers.</p>  |
| Medium (M)        | <p>When likelihood of vulnerability occurrence is of medium frequency OR ease of vulnerability exploitation by attackers with technical knowledge.</p> <p>Example:<br/>1) Exploit codes available in raw source code. Thus, attackers would require programming knowledge as well as the understanding of network infrastructure environment for the exploit to work.</p> |
| Low (L)           | <p>When likelihood of vulnerability occurrence is of low frequency OR services with no known vulnerability.</p> <p>Example:<br/>1) Exploit code unknown and not available.</p>  |

*Table 2: Likelihood Rating Matrix*

### 3.3 Summary Risk Rating

The summary risk rating is then evaluated based on both the impact and likelihood of threats. The summary risk ratings are as follows:

| Impact \ Likelihood | High   | Medium | Low    |
|---------------------|--------|--------|--------|
| High                | High   | High   | Medium |
| Medium              | High   | Medium | Low    |
| Low                 | Medium | Low    | Low    |

*Table 3: Summary Risk Rating Matrix*

### 3.4 Risk Controls Resolution Timeline

Based on the summary risk rating, we suggest the following risk controls resolution timeline:

| Risk Rating | Risk Controls Resolution Timeline  |
|-------------|--|
| High        | Immediately / During Next Maintenance Period / Resolved in less than 2 weeks |
| Medium      | Resolved in less than 4 weeks  |
| Low         | Resolved in less than 6 weeks  |

*Table 4: Risk Controls Resolution Timeline*



## 4. Test Scope

Below is a listing of the test components. It gives an overview of the areas tested. The results of these tests are explained in more detail thereafter.

| Types of tests performed  | Checked                             |
|---|-------------------------------------|
| <b>1. Certification Authority Audit</b>   |                                     |
| <ul style="list-style-type: none"> <li>▪ Interviews and discussions with appropriate stakeholders</li> </ul>                            | <input checked="" type="checkbox"/> |
| <ul style="list-style-type: none"> <li>▪ Sighted of relevant records, documentation and processes</li> </ul>                            | <input checked="" type="checkbox"/> |
| <ul style="list-style-type: none"> <li>▪ Visited the Data Centre for its implementation of the physical and logical security</li> </ul> | <input checked="" type="checkbox"/> |
| <ul style="list-style-type: none"> <li>▪ Discussion on interim findings</li> </ul>  | <input checked="" type="checkbox"/> |

## 5. Certification Authority Audit

This section attempts to determine whether in-scope applications are developed accordance to Security Guidelines for Certification Authorities Version 2.0 policies. Moreover, it shall also evaluate the security controls implemented in the application and system. Recommendations were provided to close up any non-compliance findings.

### 5.1 Physical and Environmental Controls Lapse (M)

Security Guidelines for Certification Authorities Version 2.0 Reference Number: 25, 78

#### Observation

During the course of assessment, it was observed that the following physical and environmental controls were not met:

#### DR Site

1. Cables were untidy and hidden underneath the server rack.
2. Combustible materials were kept next to the server rack.
3. Server racks were not locked at all times.
4. Although there was a camera installed to monitor user activities within the DR site, however there was no physical protections implemented to protect the camera from unauthorized removal.

#### Equinix Data Centre

1. Combustible materials were kept next to the server rack.
2. Server cabinet rear door were not locked at all times.
3. Cables were untidy.

For Equinix Data Centre, it was noted that the primary site was hosted in a private hosting centre that has multiple layer of security controls implemented including biometric access, CCTV, security screening, etc. All these controls could largely eliminate/mitigate the possibility of outsiders (e.g. vendors, auditors, etc.) from exploiting the risk. However, this control may not be sufficient to mitigate the risk of an insider attack.

#### Implication

Poorly routed cables can lead to decreased airflow and improper hardware management.

A latent risk of fire exists due to the presence of both, constant ignition source electricity and plentiful supply of combustible materials.

The lack of rack level security could potentially allow unauthorized access and criminal activity from happening.

The absence of physical security controls implemented to secure the camera would potentially allow ones to hinder the controls to deviate from its primary purpose. As a result, the footage captured by the camera may not reflect the actual activities happened within the DR site. For example: The camera which was installed at the entrance of the DR site was secured only using blu-tack. The controls were not effective in preventing unauthorized removal/replacement.

### Recommendation

We recommend the following:

- Server racks shall be locked at all times to prevent any unauthorized access.
- Proper cable management shall be enforced at all times which would aid in reducing any unnecessary time spent on identifying tangled cables.
- Monitoring devices shall be installed at areas that are non-reachable to any personnel. In addition, hardware protection shall also be implemented to prevent unauthorized from tampering with the AC and network cable.

### Management Response

Netrust would take measures to ensure that the server racks are locked. Do note that the servers are in a private suite, with access controlled by biometrics. The suite is accessible to Netrust authorized personnel only. There are already multiple layers of access control – the first layer is controlled by Equinix security staff for access to the Data Centre itself. The second layer is for access to Netrust suite, where only authorized Netrust personnel with pre-registered biometrics can access.

Surveillance camera will be upgraded and be mounted on a higher level to prevent unauthorized tampering.

## 5.2 Record Management Lapse – Records of Periodic Review Absent (L)

Security Guidelines for Certification Authorities Version 2.0 Reference Number: 9, 17, 47, 50, 77, 84

### Observation

During the course of assessment, although there was review performed for the following, however it was not being documented:

1. Monthly security management access control matrixes review
2. Quarterly job responsibilities and access matrix (logical and physical) review
3. Annual archival review
4. Alternate days audit trails review

### Implication

The lack of sufficient records to validate that the review has been conducted, could potentially lead to accountability issues. For example: If a user mentioned he has reviewed the application logs but was not documented, there could be a possibility whereby the review was not conducted. In the event whereby a security incident occurs, there will not be any records to trace who has reviewed the application logs and has he performed what is required from him.

### Recommendation

We recommend documenting records of review conducted. The documentation shall minimally include:

- Personnel who performed the review
- Personnel who validated the review was indeed conducted
- Period of the audit trails/archival/access control matrix being reviewed
- Timeline of when the review was performed
- Any security violations/security breaches being flagged.

### Management Response

Netrust will improve the recording of the reviews.

### 5.3 Documentation Management Lapse (L)

Security Guidelines for Certification Authorities Version 2.0 Reference Number: 6, 10, 12

#### Observation

During the course of assessment, it was observed that following controls were not met:

1. Documented policies/procedures resided at Equinix Data Centre were not the latest updated version.
  - a. Netrust Security Policy Version 1.6 March 2016
  - b. Netrust Public Key Infrastructure Architecture Version 2.2 March 2016
  - c. Netrust Business Continuity Plan (BCP) Version 1.0.21 March 2016
  - d. Netrust Critical Incident Response Procedures Version 1.7 March 2016
2. Documented procedures for vulnerability management were not available.
3. Although the risk assessment policy last revision history reflected was during December 2014, it was noted that there was a review conducted during January 2017 with no amendment made. However, under section 3.4 Techniques Recommendation, it was observed that the document is still referencing to the older version of OWASP Top 10 2010, and SANS Top 20.

#### Implication

The use of outdated policy and procedure manual could potentially misguide the employees in the wrong direction. As a result, this would affect the organization business in terms of consistency and efficiency.

The lack of clearly defined procedures would potentially lead to enforcement issues, whereby users may develop their own perspective of processes which may not be aligned with the organization's goals.

#### Recommendation

We recommend the following:

- Ensure a copy of the updated policies and procedure manual are resided at Equinix Data Centre at all times. Any copies of the earlier version shall be secure disposal.
- Implement documented vulnerability management procedure, where it defines how should vulnerabilities identified by automated tools are handled (Identification, Rectification, Verification).
- Revise the existing risk assessment policy to be updated with the latest references instead.

#### Management Response

All Netrust staffs are apprised of the updated policy and procedure documents. However, there is an oversight in not replacing the documents at the Data Centre with the latest. This has been rectified. For the vulnerability management, we will not create a separate document but instead enhance on the Critical Incident Response Procedures document, which would comprise of both critical and non-critical incidents. The editorial error in referencing the older version of OWASP Top 10 and SANS Top 20 had been corrected.

## 5.4 Vulnerability Management Lapse – Periodic Assessment Not Met (L)

Security Guidelines for Certification Authorities Version 2.0 Reference Number: 75

### Observation

During the course of assessment, it was observed that latest Network Penetration Test (inclusive of both network components and operating system) was conducted during January 2017. According to the Security Guidelines for Certification Authorities Version 2.0, the respective Certification Authority is required to perform the assessment on weekly basis.

Due to the application is situated in an isolated network segregated from the internet, access to production system could only be done via direct console access or remote administrative through VPN access. Remote administrative are restricted to only authorized personnel, Netrust Operations team.

With the considerations of the abovementioned factors plus there was quarterly network penetration test performed, the risk level was classified as low.

### Implication

The absence of periodic security assessment conducted could potentially overlook security weakness within the network. As a result, this would affect the organization rectification process in mitigating the issues before it can be exploited.

### Recommendation

We recommend implementing weekly vulnerability scanning to identify any security weaknesses within the network. The assessment performed has to be documented together with the rectification controls implemented to mitigate the security vulnerabilities identified.

### Management Response

Netrust will implement weekly vulnerability scanning to identify any security weaknesses within the network.

## 6. Version Control

| Version Number | Date                        | Amendments  | Author   | Reviewed By  |
|----------------|-----------------------------|---|--|--|
| 0.1            | 18 <sup>th</sup> April 2017 | Initial Draft Created                                     | Elean Kwek<br><i>Associate Security Consultant</i> | Edwina Tan<br><i>Project Manager,<br/>Senior Security Consultant</i> |
| 0.2            | 20 <sup>th</sup> April 2017 | Section 5.3 Removed.<br>Management Response Incorporated. | Elean Kwek<br><i>Associate Security Consultant</i> | Edwina Tan<br><i>Project Manager,<br/>Senior Security Consultant</i> |
| 0.3            | 21 <sup>st</sup> April 2017 | Cover Page and Sign-Off Page Amended                      | Elean Kwek<br><i>Associate Security Consultant</i> | Edwina Tan<br><i>Project Manager,<br/>Senior Security Consultant</i> |
| 0.4            | 24 <sup>th</sup> April 2017 | Section 5.2 Management Response Amended                   | Elean Kwek<br><i>Associate Security Consultant</i> | Edwina Tan<br><i>Project Manager,<br/>Senior Security Consultant</i> |
| 1.0            | 31 <sup>st</sup> May 2017   | Final Report Created                                      | Elean Kwek<br><i>Associate Security Consultant</i> | Edwina Tan<br><i>Project Manager,<br/>Senior Security Consultant</i> |

**END OF DOCUMENT**



[Home](#) > [Regulations, Licensing and Consultations](#) > [Acts and Regulations](#) >  
[Electronic Transactions Act and Regulations](#) > [Controller of Certification Authorities](#) >  
[Accredited CAs in Singapore](#)

# Accredited CAs in Singapore

LAST UPDATED 05 JULY 2017

The following company has been accredited by the Controller:

## **Netrust Pte Ltd**

### 1. Contact Details:

The Operations Manager

Netrust Pte Ltd

70 Bendemeer Road

#05-03, Luzerne,

Singapore 339940

Tel : +65 6212 1388

Fax: +65 6212 1366

Email : [infoline@netrust.net](mailto:infoline@netrust.net)

2. Netrust Pte Ltd has commenced operation as a licensed CA on 14 June 2001.

3. With the changes from the voluntary licensing scheme to a voluntary accreditation scheme for CAs, under the re-enacted 2010 ETA and 2010 ETR, Netrust Pte Ltd has been an accredited since 14 June 2011.

4. The current CA accreditation is valid for 2 years from 14 June 2017 to 13 June 2019.

### 5. CA Certificates

Netrust Root CA 1 Certificate (ZIP)

## Netrust Root CA 2 Certificate (ZIP)

### 6. Repository

- URL of repository:
- Netrust CA1 - ldap://ldap1.netrust.net
- Netrust CA2-1 - ldap://ldap21.netrust.net
- Netrust CA2-2 - ldap://ldap22.netrust.net

### 7. Certification Practice Statement and Certificate Policies

The Netrust Certificate Practice Statement and relevant Certificate Policies can be assessed at <http://www.netrust.net>

### 8. Recognised Certificates

1. Netrust Root CA Certificate
2. Netrust Signing CA Certificate
3. Netrust Personal Net-ID Certificate
4. Netrust Corporate Net-ID Certificate
5. Netrust NetServer Server Certificate

### 9. Logos For Accredited CAs

Accredited CAs may display the following logos during the conduct of their business as an indication that they have been accredited by the Controller.



The accreditation criteria are stipulated in the Electronic Transactions Act 2010, Electronic Transactions (Certification Authorities) Regulations 2010 and the Compliance Audit Checklist for Certification Authorities.

Last Updated on **05 July 2017**

Copyright © Info-communications Media Development Authority

