Introduction to Security in NC GROUP

Security Whitepaper

Created By

NC GROUP

Last Update: 12 October 2022

Table of Contents

I. Overview

NC GROUP provides various managed cloud services for our customers, no matter on Public Cloud, Multi-Cloud, Hybrid Cloud or Private Cloud.

NC GROUP strives to provide customers with consistent, reliable, secure, and compliant managed cloud services, helping customers ensure the confidentiality, integrity, and availability of their systems and data.

To help you better understand the collection of security controls implemented within NC GROUP from both the customer's and NC GROUP operation' perspectives, this white paper, 'Introduction to Security in NC GROUP', is written to provide a comprehensive look at the security available with NC GROUP.

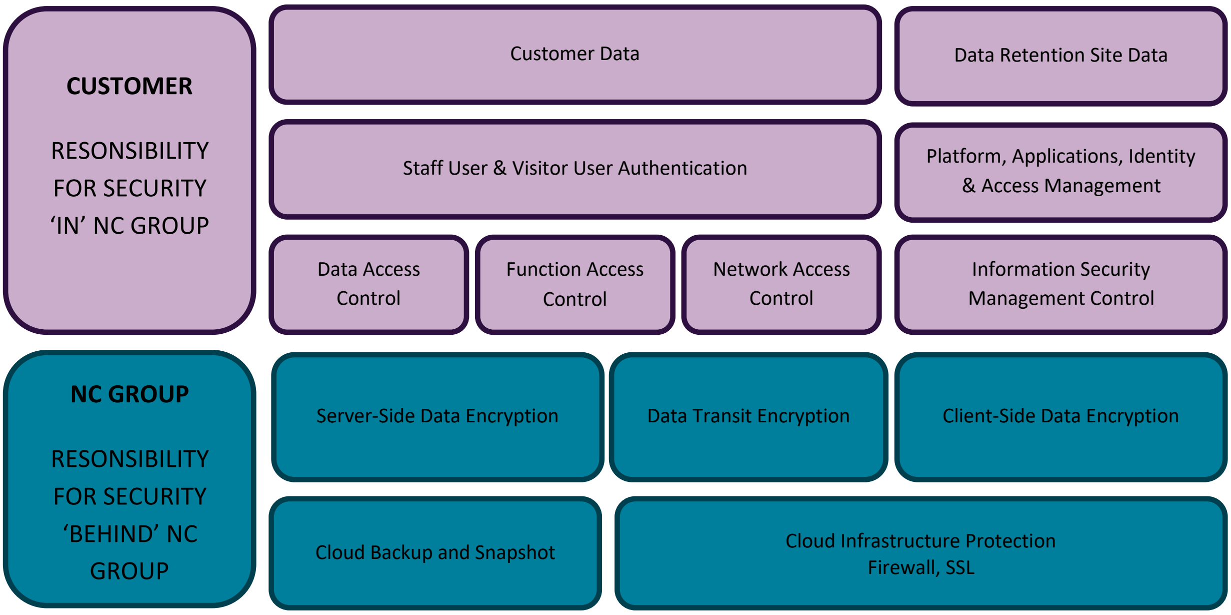
II. Role and Responsibility

2.1 Shared Security Responsibility

Security and Compliance is a shared responsibility between End User Customer and NC GROUP as the PaaS Provider.

NC GROUP responsibility "Security Behind NC GROUP " – NC GROUP is responsible for protecting the infrastructure, including data, software, hardware, networking, and facilities that run in the service.

Customer responsibility "Security in NC GROUP " – Customer responsibility will be determined by the features adopted and deployed. This determines the amount of configuration work the customer must perform as part of their security responsibilities.



CUSTOMER

RESONSIBILITY FOR SECURITY 'IN' NC GROUP

Customer Data

Data Retention Site Data

Staff User & Visitor User Authentication

Platform, Applications, Identity & Access Management

Data Access Control

Function Access Control

Network Access Control

Information Security Management Control

NC GROUP

RESONSIBILITY FOR SECURITY 'BEHIND' NC GROUP

Server-Side Data Encryption

Data Transit Encryption

Client-Side Data Encryption

Cloud Backup and Snapshot

Cloud Infrastructure Protection
Firewall, SSL

III. Infrastructure

Security and Compliance is a shared responsibility between End User Customer and NC GROUP as the PaaS Provider.

IT infrastructure is the foundation of NC GROUP's services. A robust IT service is dependent on robust IT infrastructure.

Our IT infrastructure consists of:

- Capacity Planning
- Availability Planning
- Continuity Planning
- Security Planning
- Business Growth Planning

We build our IT infrastructure with careful technical planning and business planning to ensure it fulfils industry standards and business needs.

NC GROUP also uses multiple public clouds for better service. These tier-1 data centres are all applied to local compliance.

IV. Operation Security

4.1 Staff Security

4.1.1 NC GROUP staff attends information security training and signs a non-disclosure agreement.

4.1.2 NC GROUP operation staff is required to attend a product training including managing the cloud service platform and securing customer data.

4.2 Staff Authentication Control

4.2.1 Every NC GROUP staff has own unique login account, which is used to access NC GROUP internal network and systems. Once the staff leaves NC GROUP, his/her login account will be terminated immediately.

4.2.2 Role base access control is used in NC GORUP internal network and systems. Any change or modification to the service platform must be reviewed and approved to ensure it aligns to business and operation objective.

4.3 Audit Trail

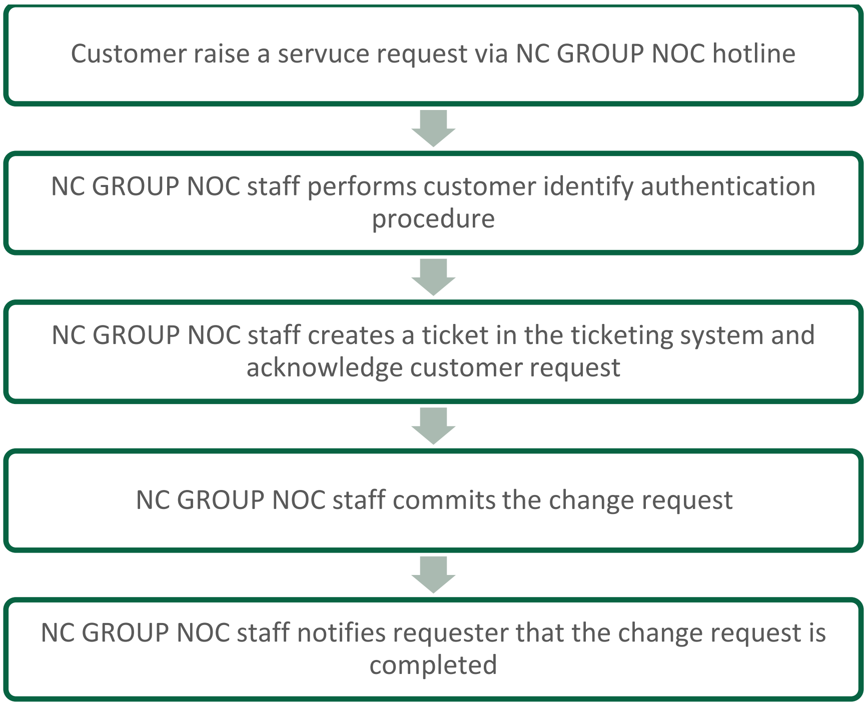
4.3.1 All activities and operation tasks in NC GROUP internal network and systems are logged in details (e.g. User ID, time stamp and action detail), which is used to track historical activities.

4.3.2 All the system logs are kept at a safe place for an enough long period, which can be retrieved if necessary.

V. Change Management

5.1 Managed Cloud Service Support Workflow

5.1.1 NC GROUP staff will never access customer's virtual machine or data without customer's permission. Only when customer initiates a service request, NC GROUP cloud operation staff will strictly follow the workflow below to process the change:



Customer raise a servuce request via NC GROUP NOC hotline

NC GROUP NOC staff performs customer identify authentication procedure

NC GROUP NOC staff creates a ticket in the ticketing system and acknowledge customer request

NC GROUP NOC staff commits the change request

NC GROUP NOC staff notifies requester that the change request is completed

VI. Data Destruction

6.1 Customer Data Destruction

NC GROUP deletes data assets of customers promptly or returns the data assets according to relevant agreements. The erasure operations are logged to prevent unauthorized access to customer data. NC GROUP staffs are not allowed to access customer data without prior consent from the customers. In line with the principle of keeping production data within the production cluster, any channels for production data to flow out of the production cluster are blocked via technical means, thus preventing O&M personnel from copying data from the production system.

VII. Security Incident Handling and Reporting

7.1 Information Security Management

7.1.1 Security incident refers to information leakage that will be undesirable to the interests of the customers or an adverse event in an information system and/or network which poses a threat to computer or network security in respect of confidentiality, integrity and availability.

7.1.2 Examples of security incidents include: unauthorized access, unauthorized utilization of services, denial of services, compromise of protected data / program network system privileges, leaks of classified data in electronic form, malicious destruction or modification of data, penetration and intrusion, misuse of system resources, computer viruses and hoaxes, and malicious codes or scripts affecting networked systems.

7.2 Security Incident Handling

7.2.1 When a security incident is detected, security incident response is made by the responsible parties following the predefined procedures. A security incident response represents the activities or actions carried out to tackle the security incident and to restore the system to normal operation that follow the severity of security incident handling base on 7.2.2 to provide latest update or information to customers.

7.2.2 NC GROUP classifies service deterioration mainly into Critical and High levels determined by NC GROUP in every single incident based on the Table 2:

Severity	Initial Acknowledgement	First Response Time	On-going Response Time	Description
Critical	30 minutes	1 hour	2 hour	Customer server/service outage (service is down)
High	30 minutes	1 hour	4 hours	Customer server/service degraded

7.2.3 Customer can report problem/fault via phone or email, escalation contact:

NOC hotline Tel: 2708 8405 Email: helpdesk@nc-s.hk

7.2.4 When the security incident is over, follow up actions will be taken to evaluate the incident and to strengthen security protection to prevent recurrence.

VIII. Vulnerability Management

8.1 Vulnerability Management Approach

8.1.1 NC GROUP follows secure development best practices, which ensure regular reviews of the effectiveness of security controls and policies, and completion of a risk assessment. NC GROUP review begins during the design phase and the engagement lasts through launch to ongoing operations.

8.1.2 NC GROUP secures infrastructure of management cloud service to protect it against attacks to guarantee the efficiency of controls against new threats and vulnerabilities.

8.1.3 NC GROUP conducts vulnerability assessment of the infrastructure of management cloud service and its components regularly to verify existing controls.

IX. Vulnerability Reporting

9.1 How to Report Vulnerabilities

9.1.1 NC GROUP takes security seriously and investigates all reported vulnerabilities. NC GROUP welcome any Staff, Customer or Contractor to report vulnerabilities in any aspect of our managed cloud services.

9.1.2 If the customer would like to report a vulnerability or have a security concern regarding managed cloud services, please send email to helpdesk@nc-s.hk.

9.1.3 If the customer suspects that NC GROUP managed cloud service's resources are being used for suspicious activity, the customer can report it to helpdesk@nc-s.hk.

9.1.4 In order for NC GROUP to respond customer's report more effectively, customer should provide any supporting material (proof-of-concept code, tool output, etc.) that would be useful in helping NC GROUP to understand the nature and severity of the vulnerability. The information customer shared with NC GROUP as part of this process is kept confidential within NC GROUP. It will not be shared with third parties without customer's permission.

9.1.5 NC GROUP will review the submitted report, and assign it a ticket number, then respond to customer, acknowledging receipt of the report, and outline the next steps in the process.

9.2 Vulnerabilities Evaluation by NC GROUP

9.2.1 Once the report has been received, NC GROUP will work to validate the reported vulnerability. If additional information is required in order to validate or reproduce the issue, NC GROUP will work with the customer to obtain it.

9.2.2 If the vulnerability is found to affect a third party product within managed cloud service, NC GROUP will notify the related third party responsible of the affected software. NC GROUP, if necessary, will coordinate between customer and the third party until the issue is resolved. Customer's identity will not be disclosed to the third party without customer's permission.

9.3 Public Notification of Vulnerabilities

9.3.1 NC GROUP will notify any validated vulnerability to the customer and to the public whereas possible.

9.3.2 In order to protect our customers, NC GROUP requests that customer shall not post or share any information about a potential vulnerability in any public setting until NC GROUP have researched, responded to, and addressed the reported vulnerability and informed customers if needed.

X. Acceptable Use Policy

10.1 No Illegal, Harmful, or Offensive Use or Content

10.1.1 Customer shall not use, or encourage, promote, facilitate or instruct others to use, managed cloud service for any illegal, harmful, fraudulent, infringing or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content including, but not limited to:

- Illegal, Harmful or Fraudulent Activities. Any activities that are illegal, that violate the rights of others, or that may be harmful to others, NC GROUP 's operations or reputation, including disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, Ponzi and pyramid schemes, phishing, or pharming.
- Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

10.2 No Security Violations

10.2.1 Customer shall not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device. Prohibited activities including, but not limited to:

- Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System;
- Interception. Monitoring of data or traffic on a System without permission; and
- Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

10.3 No Network Abuse

10.3.1 Customer shall not make network connections to any users, hosts, or networks unless the customer have permission to communicate with them. Prohibited activities including, but not limited to:

- Monitoring or Crawling. Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled;
- Denial of Service (DoS). Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective;
- Intentional Interference. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques;
- Operation of Certain Network Services. Operating network services like open proxies, open mail relays, or open recursive domain name servers; and
- Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

10.4 Monitoring and Enforcement

NC GROUP reserves the right, but does not assume the obligation, to investigate any violation of this policy or misuse of the managed cloud service. Any attempt to breach authentication or security measures by "denial-of-service" attack, port scanning and probing, any release or malicious activity of a virus or worm whether intentional or unintentional, or any unauthorized attempt to gain access to any other account, host or network is prohibited, and will result in immediate service termination, which may be without notice.

XI. Security Concerns on our Key Cloud Partner

Alibaba Cloud

https://resource.alibabacloud.com/whitepaper/alibaba-cloud-security-whitepaper---international-edition-v21-2021_1717

Google Cloud Platform

https://cloud.google.com/docs/security/overview/whitepaper

Cloudflare

https://www.cloudflare.com/trust-hub

XII. Release History

October 2022 – Version 1.0 was released

- End of document -