

NSCC Quantum User Account Management Policy

A. Document Details	
Policy Name	NSCC Quantum User Account Management Policy
Policy Owner	National Supercomputing Centre (NSCC) Singapore
Version	1.0
Author	Crispian Wong
Date Documented	January 2026

B. Approval	
Approved By:	Advanced Quantum Computing Infrastructure Working Committee
Date of Approval:	11 February 2026

1. OVERVIEW

This policy establishes the principles and framework for managing user accounts that access Quantinuum’s remote quantum system, and on-premises quantum system (collectively termed as “Quantum Systems”). It is designed to provide clear guidance on account creation, use, maintenance, and termination to ensure A*STAR Research Entities (ARES)’s compliance with the Strategic Partnership and Quantum System Access Agreement (SPA) of 5 November 2025 signed with Quantinuum Pte. Ltd, and comply with the Advanced Quantum Computing Infrastructure Letter of Award’s requirement of paragraph 4.1.c dated 23 October 2025.

It should be noted that the management of user accounts is heavily dependent on Quantinuum’s Nexus platform and its features. The policy supports a structured approach to manage user access in compliance with information security standards, operational efficiency, and Nexus’ capabilities.

2. PURPOSE

The purpose of this policy is to:

- Define standards and procedures for user account lifecycle management
- Ensure only authorised individuals have access to quantum resources
- Protect sensitive data and computational assets from unauthorised access or misuse
- Provide consistent and auditable practices for account management that align with organisational security policies and legal requirements
- Ensure users' compliance under ARES' obligations in the SPA

3. SCOPE

This policy applies to:

- All users who require or currently have access to Quantum Systems through NSCC
- All user accounts associated with access granted by NSCC through Quantinuum's Nexus platform to access Quantum Systems
- All systems, platforms, and tools within NSCC's control that support or integrate with the quantum environment

It includes all stages of the account lifecycle: request, approval, provisioning, use, modification, suspension, and termination.

4. POLICY

4.1 User Account Classification

4.1.1 User Account Roles

The roles of user accounts available are categorised based on the role and responsibilities associated with each account. The classifications are as follows:

No	Type	Description
4.1.1.1	Quantum Systems end user	Quantum Systems end users are standard users granted access to quantum resources under an approved project. They are responsible for executing computational tasks and must comply with both project-specific and system-wide policies.
4.1.1.2	System Administrator	System administrator accounts are assigned to system administrators, support personnel, and other authorised staff who perform operational, security, or user management functions. These accounts have elevated privileges and are subject to strict access controls and auditing.

Table 1: User Account Roles

4.1.2 Principal Investigators (PIs) are individuals responsible for leading the project. While PIs have similar access to quantum resources as end users from an IT perspective, they also act as the main point of contact for project-related administration. This includes managing associated users and overseeing resource usage through varied avenues, including but not limited to Nexus's Groups Tab.

4.1.3 A user account can be associated with one or more roles.

4.2 User Account Category

4.2.1 User accounts are classified into categories based on how they are created and managed. The categories are described below:

No	Category	Description
4.2.1.1	Manual Creation	Accounts in this category are manually created by system administrators via an invite to the user through Nexus, and based on approved requests by the Quantum Resource Committee.

Table 2: User Account Category List

4.2.2 A user account can only be associated with one category type.

4.3 User Account Lifecycle Management

4.3.1 The user account lifecycle encompasses the stages from initial request to final termination, ensuring proper governance, security, and compliance throughout. Each phase is described below:

No	Lifecycle Phase	Description
4.3.1.1	Account Request	The user initiates access by submitting a formal request, including personal identity details, Quantum Resource Committee's approval of the user's request for access to Quantum Systems, and signed acknowledgement of SPA's Export Control and End User Certification (see Appendix II). This marks the beginning of the account lifecycle.
4.3.1.2	Identity Verification and Approval	The user's identity and eligibility are verified by the System Administrator. Authorised personnel review the request and grant approval based on established access criteria and relevant documentation, including but not limited to US Department of Trade's Consolidated Screening List, and organisational policies.
4.3.1.3	Account Creation and Provisioning	Upon approval, the user is invited to create an user account, assigned appropriate roles, and granted access to relevant resources. Credentials and onboarding instructions are securely provided.
4.3.1.4	Active Use	The user actively engages Quantum Systems within the boundaries of their assigned roles and permissions. Ongoing monitoring ensures security, performance, and policy compliance.
4.3.1.5	Account Modification	Users may request changes to their access rights or resource allocations. All modification requests are subject to review and approval before implementation.
4.3.1.6	Account Monitoring	Account activity is continuously monitored to identify anomalies, potential security risks, or misuse. Regular audits confirm that access remains appropriate and compliant.
4.3.1.7	Account Suspension	Accounts may be suspended due to inactivity, policy violations, security incidents, or administrative decisions. Suspended users are denied access to compute resources until issues are addressed and resolved.

4.3.1.8	Account Reactivation	Previously suspended accounts can be reactivated following verification and re-approval. Access to compute resources is restored to prior roles or updated requirements.
4.3.1.9	Account Expiry	Accounts will be suspended upon the conclusion of a project, contract, or authorisation period. Access is suspended unless a formal extension is requested and approved. Access to data during the retention period will be granted based on data management policy.
4.3.1.10	Account Deactivation	When an account is no longer needed, it is permanently closed and access is fully revoked. Associated data is archived or deleted in accordance with retention and security policies.
4.3.1.11	Post-Deactivation Review	A final audit is conducted to verify complete removal of access and proper handling of user data. Removal records will be sought from Quantinum. This step ensures alignment with security, audit, and regulatory requirements.

Table 3: User Account Lifecycle Management Phases

4.4 User Account Status

4.4.1 The following describe the available status of a user account throughout the lifecycle:

No	Status	Description
4.4.1.1	Requested	The account request has been submitted by the user but has not yet been reviewed. No access is granted at this stage, and the request is pending initial validation.
4.4.1.2	Pending Approval	The account request is under review by the System Administrator. Access is not yet provisioned until formal approval is granted.
4.4.1.3	Invited	The account is created via an email invite sent to the user by the System Administrator. Access is not yet provisioned until the invite is accepted within 10 days.
4.4.1.4	Active	The user account is fully approved and provisioned with appropriate access rights. The user can log in and use the Quantum Systems.

4.4.1.5	Suspended	The account has been suspended, typically due to long-term inactivity, change in user status or critical policy violations. Access to Nexus is still permitted but access to compute resources is revoked. Data is archived or deleted in accordance with policy.
4.4.1.6	Deactivation	Associated data, such as user files and/or shared with other users, is removed. No active login or access is possible from a deactivated state.

Table 4: User Account Status Description

4.5 User Account Eligibility

4.5.1 The table below outlines the eligibility criteria for each category of user account:

No	Category	Account Eligibility
4.5.1.1	Manual Creation	<ul style="list-style-type: none"> Requestors must fall under one or more of the user account types defined in Section 4.1.1. Eligibility is subject to the Quantum Resource Committee's approval, and the System Administrator's review, including signed compliance with applicable export control laws and regulations, and end-user certification. Only users with valid organisational email addresses are eligible for manual account creation. Personal emails are not allowed.

Table 5: User Account Eligibility

4.6 User Account Creation, Extension and Modification Approval Matrix

4.6.1 For user accounts classified under the "Manual Creation" category, approval must be granted by the designated authority(ies), as specified below:

No	Roles	Approving Authority(ies)
4.6.1.1	Quantum end user	Quantum Resource Committee, NSCC System Administrator
4.6.1.2	System Administrator	NSCC

Table 6: User Account Creation, Extension and Modification Approval Matrix

4.6.2 For users with existing email accounts requiring migration to ARES SPA organisation in Nexus, intervention by the Quantinuum Administrator via QCsupport@quantinuum.com is required. The System Administrator's consent shall be obtained prior to Quantinuum proceeding with the migration.

4.7 User Account Information

4.7.1 For user account which falls under category of “Manual Creation”, the following information, along with supporting documentation, is collected:

- a. First name
- b. Last name
- c. Nationality
- d. Country of residence during use of Quantum Systems
- e. Name of Organisation
- f. Department
- g. Designation
- h. Official Email Address

4.8 User Account Validity

4.8.1 The table below outlines the validity period for each user account category:

No	Category	Validity Period
4.8.1.1	Manual Creation	<p><u>Quantum Users</u></p> <ul style="list-style-type: none"> • Valid until the project's latest end date + 60 days <p><u>System Administrators</u></p> <ul style="list-style-type: none"> • Based on role assignment duration by NSCC

Table 7: User Account Validity Period

4.9 User Account Inactivity and Expiry

4.9.1 User accounts that remain unused for 120 consecutive days will be flagged as inactive.

4.9.2 Users will be notified via email to explain the reasons for inactivity. Failure to provide a response or providing inadequate reasons, may lead to account suspension.

4.9.3 All user accounts will be suspended at the end of their validity. These accounts will lose access to quantum resources until they are reactivated or extended.

4.10 User Account Extension and Reactivation

4.10.1 The table below outlines the extension option for each account category:

No	Category	Extension and Reactivation Options
4.10.1.1	Manual Creation	<p><u>Quantum Users</u></p> <ul style="list-style-type: none"> Validity beyond the project duration may be extended upon submission and approval of an extension request, and substantiated through relevant supporting document(s) from the Quantum Resource Committee

Table 8: User Account Extension Option

4.11 User Account Suspension and Deactivation

4.11.1 Accounts may be disabled temporarily due to prolonged inactivity, pending investigation of security incidents, or administrative decisions. Disabled accounts retain their data and configuration but are restricted from accessing any resources.

4.11.2 Suspension must be carried out by authorised administrators. Users will be notified of the reason for the action and, where applicable, the procedure for reactivation.

4.11.3 User accounts will be suspended or deactivated under any of the following conditions:

- a. End or termination of project or contract with no further need for access.
- b. End of user employment, and/or request from user's employer.
- c. Serious policy violations or security breaches.

4.11.4 Upon deactivation, associated user data may be archived, transferred, or deleted based on data retention policies.

4.11.5 All account deactivation must be reviewed to ensure complete removal of access rights. An audit record of the deactivation must be maintained for compliance and traceability. These records shall be provided by Quantinum to the System Administrator upon request.

4.12 User Account Authentication

- 4.12.1 All user accounts must be associated with a unique username and securely managed authentication credentials.
- 4.12.2 Authentication must be performed using only approved and secure methods.
- 4.12.3 Passwords must meet minimum complexity standards set by Nexus.
- 4.12.4 Users are responsible for keeping their authentication credentials secure and must not share, reuse, or store them. Compromised credentials must be reported and reset immediately.

4.13 User Account Access Control

- 4.13.1 Access to systems and resources must be based on predefined roles that reflect the user's job function or project role. Users are granted only the minimum privileges necessary to perform their duties.
- 4.13.2 Access to the Quantum Systems must be explicitly granted based on the Quantum Resource Committee's approval. Unaffiliated users may not access project-specific data or resources.
- 4.13.3 Access must be granted for a defined period aligned with the project duration or employment contract.
- 4.13.4 Access rights must be reviewed according to the following frequency:

No	Roles	Frequency
4.13.4.1	Quantum End User	Bi-Annually
4.13.4.2	System Administrator	Bi-Annually

Table 9: User Account Access Right Review Frequency

- 4.13.5 Access must be revoked promptly when it is no longer required, or upon user departure, role change, or project completion.
- 4.13.6 The Principal Investigator (PI) is fully responsible and accountable for all project members' access to project resources. The PI must ensure that only authorised users are granted access and must submit a duly signed membership modification request for any addition, removal, or change in project membership. This includes timely updates to reflect changes in project staffing or user eligibility.

4.14 User Account Usage Guidelines

- 4.14.1 User accounts must only be used for approved activities directly related to assigned projects or job responsibilities. Use of quantum resources for unlawful or prohibited activities is strictly forbidden.
- 4.14.2 Each user is accountable for actions performed using their account. Users must ensure their activities do not compromise the security, performance, or availability of the Quantum Systems.
- 4.14.3 Users must manage their resource usage responsibly and in accordance with project quotas and fair usage policies. Excessive or abusive use may lead to account restriction.
- 4.14.4 All users must comply with institutional policies, data protection regulations, and applicable legal or contractual obligations.

4.15 User Account Monitoring and Audit

- 4.15.1 All user account activities, including logins, job submissions, and administrative actions, must be logged for auditing and security purposes.
- 4.15.2 User activities will be monitored to detect unauthorised access, unusual behaviour, or policy violations.
- 4.15.3 Audits of user accounts and access rights will be conducted every six months to ensure compliance with policies and to identify inactive, expired, or misconfigured accounts.
- 4.15.4 Any suspected misuse or breach of account policy will be investigated promptly. Users may be contacted for clarification or required to participate in the investigation process.

4.16 Acceptable Use

- 4.16.1 All users and their employers must agree to comply with the following terms in order to access and use Quantinum's Remote Quantum Systems and/or On-Prem Quantum System ("the Quantum Systems"). By accessing and operating the

Quantum Systems, all users and their employers are deemed to have agreed to, and shall be bound by the terms herein.

- i All users and their employers shall adhere to the Nexus Terms and Conditions as set out in the following link, and as updated from time to time:
https://nexus.quantinum.com/auth/terms_and_conditions/current/
- ii Users understand that access to and use of the Quantum Systems are made available via Quantinum's cloud-based Nexus Platform, or such other equivalent platform. Such access is provided as a service, and may be updated or sun-setted by Quantinum from time to time provided there are sufficient systems for use. Users understand that the systems are controlled by Quantinum and may be updated, changed, or modified by Quantinum without prior notification.
- iii Once access is granted, users may place their job(s) in a queue for processing. Processing shall be subject to Fair Queuing as provided for in the Appendix I.
- iv Users shall not remove, modify, or obscure any intellectual property rights notices on the Quantum Systems or related documentation.
- v Users must: (a) implement and maintain policies and procedures reasonably designed to maintain the confidentiality of usernames, passwords, or other credentials; (b) not knowingly allow unauthorised users to use your credentials or access your account; (c) promptly notify NSCC and Quantinum of any known unauthorised use or breach of security related to their accounts; and (d) maintain and promptly update user information if it changes. If NSCC believes or is notified that a user is violating or has violated the terms and conditions of this NSCC Quantum User Account Management Policy, NSCC's Acceptable Use Policy (AUP), or the Nexus Terms and Conditions, NSCC and/or Quantinum may use reasonable management features (e.g., lockout) to prevent unauthorised use.
- vi Users represent that they are not, and their employers warrant that their employees who are users are not individuals or entities included in the U.S. Department of Trade's Consolidated Screening List available at <https://www.trade.gov/consolidated-screening-list>. Users shall not: (a) copy all or any portion of the Quantum Systems; (b) decompile, disassemble, or otherwise

reverse engineer the Quantum Systems, or any portion thereof, or determine or attempt to determine any source code, algorithms, methods, or techniques used or embodied in the Quantum Systems or any portion thereof; (c) modify, translate, or create any derivative works or improvements based upon the Quantum Systems, including by making machine code human readable; (d) interfere with the Quantum Systems's security or operation (including probing, scanning or testing the vulnerability of any security measures or misrepresenting transmission sources); (e) create, benchmark or gather intelligence for a competitive offering or competitive purposes; (f) unless otherwise agreed in writing by Quantinuum transfer the Quantum Systems to any site other than the Facility; (g) introduce, transmit, or store malicious code, Trojan horse, self-replicating, or other computer instructions that may: (i) alter, destroy, inhibit, or discontinue the Quantum Systems; or (ii) bypass or disable any internal security measure to obtain access to any Quantinuum resource(s); (h) use the Quantum Systems to introduce, transmit, or store any code that may be used, in whole or in part, for compromising any encryption; (i) infringe on a third party's intellectual property rights; or (j) use the Quantum Systems for any military, defense, or warfare-related purpose, which includes, but is not limited to, the development, production, or deployment of weapons, military equipment, or any other activities associated with armed forces or defense organisations. Further, users represent and warrant compliance with all applicable laws, and use of the Quantum Systems only for lawful purposes. Without limiting the foregoing, users represent that they will not access the Quantum Systems from, or provide or otherwise enable or permit access to the Quantum Systems by any permanent residents of, Cuba, Iran, North Korea, Russia, Syria, The Crimea Region of Ukraine, The so-called Luhansk People's Republic, The People's Republic of China (which includes Hong Kong, Macau, and its special administrative regions), and The People's Republic of Donetsk ("**Restricted Countries**"). In addition, users' employers shall submit to NSCC the signed form set out in the Appendix II. Furthermore, users shall not access the Quantum Systems from Qatar.

- vii* Open-source software ("**OSS**") may be used in the Quantum Systems and to the extent required by the licenses covering OSS, the terms of such licenses will apply to users' use of the OSS. If, and solely to the extent the licenses applicable to OSS: (a) prohibit any restriction with respect to such OSS, such restriction will

not apply to such OSS and (b) require us to make an offer to provide source code or related information in connection with the OSS, such offer is hereby made, in each case, solely with respect to the corresponding OSS which is governed by such OSS license.

- viii Users shall not disparage the name, trademark or proprietary indicia of NSCC, A*STAR, or Quantinuum or any subsidiary or affiliate thereof. Users shall not make statements or representations, or otherwise communicate, directly or indirectly, in writing, orally, or otherwise, or take any action which may, directly or indirectly, disparage NSCC, A*STAR, or Quantinuum, their affiliates, their business or their officers, directors, employees, advisors, products, services, businesses or reputations. Notwithstanding the foregoing, nothing in this Agreement shall preclude User from making truthful statements that are required by applicable laws, regulation, or legal process.
- ix User agrees that NSCC and/or Quantinuum shall not be in default, if failure to perform any obligation hereunder is caused solely by events or conditions beyond their reasonable control, including acts of God; cyberattack; loss of third party vendors' services or supplies, unavailability of public internet and communications network; fire; explosion; extreme flood; extreme tropical storms; hurricanes; tornadoes; severe weather conditions; earthquakes; major electrical failures, supply chain shortages or delays (including an inability to secure an adequate supply of liquid helium); acts of civil commotion; strikes; war(whether an actual declaration thereof is made or not); pandemics; sabotage; insurrection; action of a public enemy; failure in transportation; law or regulatory change; judicial action; or governmental demands or requirements or the absence of government approvals all of which are beyond such affected party's commercially reasonable control (each instance a "Force Majeure Event") in each case, so long as such failure to perform could not have been prevented by reasonably foreseeable and reasonable precautions.
- x User shall have obtained all necessary approvals and clearances from third party rightsholders prior to ingestion of any data and instructions input, uploaded, transmitted, or made available by NSCC or its licensors into the Quantum Systems, including associated algorithms either in their original form or any modified form, for use in transferring, composing, and processing provided data ("Input Data").

- xi User shall not use the Input Data except for the purposes of using the Quantum Systems and shall not disclose this to any third party without the prior written consent of NSCC or its licensor.

4.16.2 This NSCC Quantum User Account Management Policy will be published and made available online.

5. CONFIDENTIALITY

5.1 Users shall not accept any information marked "Confidential and/or Proprietary" pertaining to the Quantum Systems from any third party without NSCC's prior written approval. Users must immediately inform NSCC should they receive any such information, and must not disseminate it.

6. REVISION HISTORY

Version	Date Issued	Revised By	Brief Summary of Changes
1.0			First version of document

APPENDIX I: FAIR QUEUING

When users access the Quantum Systems, users' jobs will be processed alongside jobs from other users according to Quantinuum's "**Fair Queuing System**". The Fair Queuing System is designed to ensure that each organisation with access to the Quantum Systems gets a "fair share" of the queue and is not blocked out by other organisations.

The Fair Queueing System is weighted by subscription level.

The Fair Queueing System has the following specifications and functions:

- The Quantum System(s) automatically run(s) frequent calibrations to ensure optimal performance. Submitted jobs are partitioned into segments, where the number of shots (each shot being a singular circuit of a job) in each segment, is selected to allow for the optimal calibration schedule.
- The fair queueing window is a defined time period for comparing system utilisation across each individual Remote Quantum System.
- During each fair queueing window, the partial cost of each completed segment is divided by that organisation's monthly HQC allocation and added to a fair queueing accumulator.
- The next segment processed on the Remote Quantum System is selected by giving priority to the organisation with the lowest fair queueing accumulator.

APPENDIX II: EXPORT CONTROL AND END-USE CERTIFICATION

EXPORT CONTROL AND END-USE CERTIFICATION

The products (“Products”) of Quantinum Pte. Ltd. and its affiliates (collectively “Quantinum”) are subject to U.S. and other countries' export control regulations. In accordance with such regulations, and in order to access the Products, [Party Name] provides the following assurances and undertakings to Quantinum and A*STAR Research Entities (“ARES”):

1. We understand that the Products are subject to U.S. export control regulations and/or export or import regulations in Singapore and other countries and agree to abide by all applicable export control regulations with respect to the Products and understand that we may be subject to fines and penalties for noncompliance with such laws and regulations.
2. The employer of the end-user of Products, is [Party Name], an entity whose offices are situated at: [Party's Address]. We assume all responsibility to Quantinum, ARES, their affiliates and their employees, members and representatives for all costs, damages, awards, penalties, expenses and other amounts arising out of or relating to our end-users' use of the Products.
3. We are not on the U.S. Department of Trade's Consolidated Screening List (available at <https://www.trade.gov/consolidated-screening-list>) (“CSL”).
4. We will not permit access to the Product by any person who is on the CSL or any permanent resident of, the following jurisdictions: Cuba, Iran, North Korea, Russia, Syria, The Crimea Region of Ukraine, The so-called Luhansk People's Republic, The People's Republic of China (including Hong Kong and Macau), and The People's Republic of Donetsk.
5. We will not permit access to the Product by any person located in Qatar.
6. We will not, except as specifically authorised by U.S. or other applicable government regulation or export license:
 - a. use or transfer any Products for use in the design, development, fabrication, or testing of nuclear weapons or explosive devices; or design, construction, fabrication, or operation of facilities or components of facilities for chemical processing of irradiated special nuclear or source material, heavy water production, separation of isotopes of source and special nuclear material, or fabrication of nuclear reactor fuel containing plutonium, or unsafeguarded nuclear facilities;
 - b. use or transfer any Products for use in the design, fabrication, operation, or maintenance of certain rocket systems (including ballistic missile systems, space launch vehicles, and sounding rockets); or unmanned air vehicle systems (including cruise missile systems, target drones, remotely piloted vehicles, and reconnaissance drones);
 - c. use or transfer any Products for use in the design, development, production, stockpiling or use of chemical or biological weapons;

- d. use or transfer any Products in support of deepwater (greater than 500 feet), Arctic offshore, or shale exploration or production projects that have the potential to produce oil and which involve any Russian entity that is subject to Executive Order 13662, Directive 4, as amended by Countering America's Adversaries Through Sanctions Act (Aug. 2, 2017; 131 Stat. 886).
- e. transfer, or facilitate the transfer of any Products to any person, entity, organisation or other party identified on a U.S. government-issued restricted party list, including but not limited to the U.S. Department of Commerce's Entity List, Unverified List or Denied Persons List; the U.S. Department of Treasury's Specially Designated Nationals and Sectoral Sanctions Identifications lists; or the U.S. Department of State's Nonproliferation Sanctions list;
- f. transfer, or facilitate the transfer of any Products to any U.S. sanctioned or embargoed country including but not limited to the geographic area of Crimea, China, Cuba, Iran, North Korea, Russia, Sudan or Syria.
- g. re-export any technology controlled for national security reasons by the U.S. Department of Commerce, Bureau of Industry and Security (BIS) Commerce Control List (CCL) to any destination, or export the direct product of the technology, directly or indirectly, to a country listed in Country Group D:1, E:1, or E:2 (see Supplement No. 2 to part 740 of the EAR);
- h. otherwise re-export, resell, transfer, or make other dispositions of any Products, except in accordance with the provisions of this Certification and all applicable export control and sanctions laws and regulations, as amended from time to time.

I certify that: (a) all of the facts contained in this assurance are true and correct to the best of my knowledge and belief, (b) we will adhere to the conditions detailed herein, and (c) I have the lawful authority to sign this document on behalf of the below listed entity.