IGUAKO CAPITAL · Group policy

Information Security

This policy sets the controls that protect the confidentiality, integrity and availability of the group's information and systems in all 36 offices and on every hosted platform the group uses. It classifies information into four tiers, fixes the access, encryption, patching and testing standards for each, defines how security incidents are graded and escalated, and applies the Ethical Technology Charter to the security function itself: every automated security control has a named owner, and monitoring of staff is limited to what the control requires.

CODE	CATEGORY	VERSION
IGC-DT-002	Data and technology	3.3
EFFECTIVE	**REVIEW**	**OWNER**
2022-11-01	Annual, and after any severity 1 incident. Next review due November 2026.	Chief Information Security Officer

1. Purpose, scope and accountability

The group holds client identities, transaction records, positions, research and the design of its own models. Loss or corruption of any of these would harm clients, counterparties and the group itself. This policy exists to prevent that loss, to detect quickly any loss that occurs and to restore the affected service within the objectives set in the Business Continuity and Disaster Recovery policy.

It applies to every system the group owns, every hosted service it contracts, every device that connects to the group network and every person who uses them, including contractors and third-party staff with access. The Chief Information Security Officer owns the policy and reports to the Head of Technology and Ethics, with a direct line to the Chief Risk Officer and the Audit Committee on any matter the officer considers unresolved.

Each system has a named system owner who answers for its security configuration and for the access granted to it. The list of systems and owners is the system register, held by the security function and reviewed each quarter. A system with no named owner is disconnected from the network until one is appointed. This is the first Charter principle, human accountability, applied to infrastructure.

2. Information classification

Information is classified into four tiers at the point of creation or receipt. Public information may be released without approval. Internal information is available to all staff and may not be released outside the group without the owner's approval. Confidential information is restricted to named roles and includes client records, positions, transaction pipelines and unpublished research. Restricted information is available to named individuals only and includes inside information, model source code, cryptographic keys and security configurations.

The classification determines the control set. Confidential and Restricted information is encrypted at rest and in transit, may not be stored on portable media, may not be sent to a personal address or to a public generative service, and is watermarked when rendered for printing. Restricted information is additionally held in segregated systems with dual-authorised access and is never copied to a regional hub.

The classification of a document or dataset may be raised by anyone and lowered only by its owner. Information received from a client or counterparty is treated as Confidential unless the sender has marked it otherwise. Information received under the Information Barriers and Inside Information policy is Restricted from the moment it crosses the wall.

- Public: releasable without approval.
- Internal: all staff; no external release without the owner's approval.
- Confidential: named roles; encrypted; no portable media; no public services.
- Restricted: named individuals; segregated systems; dual-authorised access; no regional copy.

3. Access control and identity

Access is granted on the principle of least privilege: a person receives the access their role requires and nothing more. Access requests are approved by the line manager and the system owner and are provisioned through the identity platform, never by direct configuration of a system. Access ends automatically on the day a person leaves or changes role, and the leaver's manager confirms the removal within five business days.

Every remote connection and every privileged action requires multi-factor authentication. Privileged accounts are separate from ordinary user accounts, are held by 41 named administrators across the group, and are reviewed monthly by the security function. All other access is recertified quarterly by the system owner, who must confirm each user individually. Recertification that is not completed within 20 business days results in suspension of the uncertified accounts.

Shared accounts are not permitted on any system that holds Confidential or Restricted information. Service accounts are owned by a named person, have no interactive login and have their credentials rotated every 90 days. Third-party staff receive access for a fixed period tied to their engagement and are subject to the same recertification as employees.

4. Technical controls

All data is encrypted in transit between offices, hosted platforms and counterparties, and at rest on every server, database and endpoint. Encryption keys are generated inside the group's key management service, rotated annually, and held under split custody so that no single person can recover a key alone. Endpoints are managed centrally, are encrypted, and are wiped remotely when reported lost.

Vulnerabilities are graded on discovery. Critical vulnerabilities on internet-facing or Restricted systems are remediated within 7 days, high within 30 days, medium within 90 days and low within 180 days. Where a fix cannot be applied within the period, the system owner records a compensating control and the Chief Information Security Officer approves a dated exception. Nine exceptions were open at 30 June 2026, none older than 60 days.

The group network is segmented so that trading, client data, corporate and guest traffic do not share a segment. Outbound traffic to public generative services is blocked at the group boundary. Email and web traffic are filtered for malicious content. Security logs from every system are collected centrally, retained for 24 months and monitored around the clock by the security operations team in Singapore and Luxembourg,

working in alternating shifts.

Automated controls that block, quarantine or disconnect are used only where the cost of a wrong block is understood and reversible within an hour. This is the second Charter principle, proportionate automation. Every automated control has a named owner, a documented false-positive rate and a manual override. A control whose false-positive rate exceeds the documented tolerance for two consecutive months is switched to alert-only until it is retuned.

5. Testing and assurance

An independent penetration test of the external perimeter and of the client reporting platform is commissioned every year, and of any new system or material change before it enters service. Findings are graded on the same scale as vulnerabilities and remediated to the same timetable. The test report goes to the Audit Committee, which sees the findings and the remediation status, not a summary.

Phishing simulations run quarterly for all staff. Any person who fails two consecutive simulations completes a supervised training session with the security function. Security awareness training is completed by every member of staff within one month of joining and annually thereafter; completion was 100 per cent of 312 people at 30 June 2026. Systems developed inside the group follow the secure development standard, including code review by a second developer and automated dependency scanning before release.

6. Security incidents

A security incident is any event that compromises or threatens the confidentiality, integrity or availability of group information or systems. Incidents are graded on discovery. Severity 1 is an incident affecting a Tier 1 service under the Business Continuity policy, a confirmed loss of Confidential or Restricted data, or an attacker with privileged access. Severity 2 affects a Tier 2 service or involves suspected but unconfirmed data loss. Severity 3 and 4 are contained events with no data loss and no service effect.

A severity 1 incident is reported to the Chief Information Security Officer immediately, to the Executive Committee within four hours and to the Chair of the Board within 24 hours. Where personal data is involved, the Group Data Protection Officer is informed at the same time as the Executive Committee and the Data Protection and Privacy policy timetable runs in parallel. Clients whose data or service is affected are told within one business day of confirmation.

Every incident of severity 2 or above is followed by a written review within 20 business days that states the cause, the timeline, the control that failed or was absent and the action taken. The review is presented to the Risk & Valuation Committee. In the twelve months to 30 June 2026 the group recorded no severity 1 incident and four severity 2 incidents, with a mean time to containment of five hours.

- Severity 1: Executive Committee within four hours, Board Chair within 24 hours.
- Affected clients informed within one business day of confirmation.
- Written review within 20 business days for every severity 2 or above incident.

Key controls

- System register naming an accountable owner for every system, with disconnection of any system lacking one.
- Four-tier classification with encryption, media and transmission controls tied to each tier.
- Least-privilege provisioning through the identity platform, quarterly recertification and monthly privileged-account review.

- Multi-factor authentication on every remote connection and privileged action.
- Vulnerability remediation at 7, 30, 90 and 180 days by grade, with dated exceptions approved by the Chief Information Security Officer.
- Central log collection retained 24 months and monitored around the clock from Singapore and Luxembourg.
- Annual independent penetration testing with findings reported in full to the Audit Committee.
- Incident grading with fixed escalation times and a written review within 20 business days.

Related policies

- Data Protection and Privacy (IGC-DT-001)
- Business Continuity and Disaster Recovery (IGC-DT-007)
- Third-Party Risk and Outsourcing (IGC-DT-006)
- Records Management and Retention (IGC-DT-003)

Colophon