AUSTRIAN GEORGIAN DEVELOPMENT LLC
(AGD LLC)

Information Security Policy

This Compliance Policy is Approved by the General Director: Giorgi Abramishvili

2025

Contents

Austrian Georgian Development LLC
Information Security Policy

Introduction

Austrian Georgian Development LLC (AGD LLC) was established in June 2013 and owns and operates hydropower projects in Georgia. The company developed the Lakhami HPP Cascade, consisting of Lakhami 1 and Lakhami 2 Hydropower Plants, located on the Lakhami River in Mestia Municipality. These run-of-the-river plants have a combined installed capacity of 16 MW and generate an average of 80 million kWh annually. The Lakhami HPPs are connected to the national grid via a 35/6 kV power transmission line.

Austrian Georgian Development LLC is co-owned by CCEH Hydro III LLC – Part of Caucasus Clean Energy Holding (CCEH), an international investment holding company founded in 2015, with investors from Western Europe and the United States, actively engaged in the Georgian energy sector. Geo Hydro Capital Group LLC – Founded in 2013, specializing in the development of small and medium-sized hydropower plants in Georgia. Energy Solutions LLC – Established in 2014, focusing on the construction and development of small and medium-sized hydropower plants, as well as providing consultancy services in the hydro energy sector.

Purpose

The purpose of this Information Security Plan (ISP) is to formalize the company's approach to safeguard its information assets, operational technology systems, and personnel data. It covers all digital and physical information handled by the company and includes provisions related to IT infrastructure, control systems (e.g., SCADA), communications, and third-party data management. This ISP applies to all employees, contractors, service providers, and any third party – such as consultants, auditors, regulators, lenders, or partners – who have access to AGD LLC's information, systems, or infrastructure. It integrates content and obligations from the Compliance Policy, including obligations to maintain confidentiality, secure systems, report breaches, and comply with national and international legal standards.

Information Security

Austrian Georgian Development LLC defines information security as the ongoing protection of the confidentiality, integrity, and availability of its data, systems, and infrastructure. This applies not only to digital systems but also to physical assets, operational technologies, and all records – whether stored on-site, in cloud platforms, or managed by external service providers. The company considers information security to be a foundational element of sustainable operations, as it directly supports compliance with legal obligations, the protection of sensitive project data, and the trust of partners, regulators, and investors.

Recognizing the strategic importance of secure information handling in the energy and infrastructure sectors, AGD LLC develops and maintains its information security practices in line with internationally accepted good practices and sectoral standards, including those applicable to critical infrastructure. These practices are tailored to the company's size, operational context, and reliance on digital technologies for both administrative and technical functions.

Information security at AGD LLC is not treated solely as a technical issue. It encompasses a wide range of risk-aware management activities, including access control, employee awareness, physical facility security, procedural discipline, and continual assessment of system vulnerabilities. The company adopts a layered approach to defense and ensures that its practices evolve alongside changes in technology, regulation, and operational risk exposure.

Information Security Governance

Information security governance at AGD LLC is led by the Company General Director, with internal coordination supported by the ESG manager. While strategic responsibility remains with the company's executive leadership, the day-to-day implementation of technical controls and cyber defenses is delegated to a qualified third-party IT and cybersecurity service provider operating under a contractual agreement.

As an operational hydropower plant operator, Austrian Georgian Development LLC recognizes that information security is a core element of regulatory compliance, system reliability, and stakeholder trust. Governance of information security reflects this strategic importance and is structured to ensure full

accountability, clarity of roles, and consistent application of good practices across all functions. Governance activities are designed not only to protect data but also to ensure operational resilience and legal alignment in a dynamic regulatory and risk environment.

Austrian Georgian Development LLC takes a comprehensive and risk-based approach to data privacy and cybersecurity. It ensures that personal and operational data are processed lawfully, fairly, and for legitimate purposes, in line with the Law of Georgian on Personal Data Protection. The company applies strict retention and access rules and ensures that individuals are informed of their data rights. Special category data, such as medical information, is processed only with appropriate legal basis or written consent. Governance structures ensure principles are upheld in both policy and practice.

Cybersecurity governance includes a structured set of technical and procedural safeguards, such as:

- Deployment and regular updating of antivirus and anti-malware software;
- Use of strong passwords and enforcement of multi-factor authentication (MFA);
- Secure data backups stored in the cloud and tested for integrity;
- Roles-based access controls with individual credentials and workstation-level protections;
- Enforcement of clean desk protocols and use of secure communications;
- Scheduled reviews of the cybersecurity program by the external IT provider to address evolving threats

The information security policy framework is reviewed on an annual basis or in response material changes in legislation, system architecture, or risk exposure. Typical triggers include software updates, commissioning if new operational tools, onboarding of third-party vendors, or amendments to the legal obligations around data management. Updated policies are formally approved by the Company General Director and circulated internally for awareness and compliance, followed by training or tool box talks.

Key reporting and governance mechanisms include:

- **Immediate escalation of any data breach or cybersecurity incident**, particularly those affecting SCADA systems, operational control networks, or sensitive data to the Company General Director and ESG Manager. Such incidents are followed by prompt documentation, root cause assessment, and coordination with the third-party IT provider to ensure effective mitigation and system recovery. This is a critical step in ensuring uninterrupted plant operations and compliance with data protection obligations;
- **Periodically performance and compliance reviews conducted jointly with the IT provider**, focused on indicators highly relevant to hydropower plant operations. These include access log audits for control systems, threat detection summaries, patching and update status, system integrity checks, and any anomalous activity within plant monitoring platforms. Regular reviews help maintain system resilience and reduce operational vulnerabilities, especially in environments where operational technologies and IT systems converge;
- **Annual ESG compliance reporting,** which includes a dedicated section addressing cybersecurity measures and information security practices. This report summarizes system-level improvements, audit results, incidents (if any), training outcomes, and alignment with national law and internationally recognized good practices. As Austrian Georgian Development LLC operates within the energy infrastructure sector, transparent ESG reporting on digital and operational resilience enhances stakeholder trust, supports financing requirements, and ensures readiness for regulatory inspection or grid integration oversight.

The third-party IT provider is required to adhere to contractual standards for security, including access enforcement, encryption, patching, and incident response. Their performance is evaluated regularly as part of the company's risk management and compliance structure.

Strategic oversight is maintained by the Company General Director, ensuring that information security is embedded into broader decision-making processes and reflects the company's commitment to legal compliance, operational continuity, and good governance.

Information Security Policy

AGD LLC has established a comprehensive Information Security Policy designed to protect its digital infrastructure, personal and operational data, and plant-specific technologies such as SCADA systems. The policy is structured to meet both national legal obligations under the Law of Georgia on Personal Data Protection and widely recognized international standards and practices applicable to critical infrastructure and energy sector operations.

As an HPP operator, AGD LLC recognizes that its information security responsibilities extend beyond internal operations to encompass employees, contractors, third-party service providers, and other entities with access to the company's systems. The policy outlines both preventive and responsive controls and reflects the company's commitment to legal compliance, operational continuity, and stakeholder trust.

Austrian Georgian Development LLC maintains a cybersecurity program aimed at preventing unauthorized access, loss, or misuse of personal and operational data. The program is implemented in coordination with a trusted third-party IT provider and includes the following safeguards:

- Regular use and updating of antivirus and anti-malware software;
- Enforcement of strong, unique passwords and multi-factor authentication (MFA);
- Data backups with secure cloud storage;
- Controlled access system, with unique employee credentials;
- Workstation security policies, including password enforcement and automatic screen locking;
- Confidentiality protocols such as clean desk practices and secure communication channels
- Periodic reviews of security policies, system configurations, and user access privileges

AGD LLC also applies strict measures to protect physical information, including printed documents, operational logs, and hardcopy records. All sensitive or confidential physical records must be stored in locked cabinets or controlled-access archives, accessible only to authorized personnel. The company enforces a clean desk policy across all administrative and operational locations, requiring employees and contractors to clear desks of documents containing confidential or personal data with those not in use. Physical records that are no longer needed must be disposed of using secure methods, such as shredding, in accordance with internal data retention and destruction policies.

In accordance with the Compliance Policy, all employees, contractors, and third-party personnel are required to sign confidentiality agreements and adhere to IT usage policies as a condition of access to any AGD LLC system or facility. These agreements are legally binding and establish clear responsibilities for data handling, system use, and ethical conduct. Violations of the information security policy – such as unauthorized access attempts, sharing of credentials, or use of non-approved software – are subject to internal investigation and disciplinary action, which may include contract termination.

The company's SCADA systems, which control and monitor real-time HPP functions, are physically and logically isolated from the public internet. Access to these systems is limited to designated technical personnel with operational responsibility and is conducted under tightly controlled conditions. Any access or update to SCADA environments is logged and reviewed by both internal management and the IT service provider.

AGD LLC also maintains a robust approach to data privacy and personal information handling. Personal data collected and processed – such as contact, financial, behavioral, and technical information – is stored securely and retained only for as long as necessary to fulfill its business or legal purpose. Access to such data is restricted according to role-based permissions, and any disclosure or processing of special category data (e.g., health-related information) is performed only with a valid legal basis or documented consent. Video

surveillance conducted at operational sites is limited, proportionate, and visibly signposted in line with applicable data protection regulations.

Austrian Georgian Development LLC maintains formal internal retention and deletion procedures. Data no longer needed is either securely deleted, anonymized, or archived, unless specific legal obligations (e.g., tax, environmental) require continued retention.

Through these policy measures, AGD LLC ensures that its information systems, operational technologies, and personal data assets are protected from unauthorized access, misuse, or loss – thereby supporting its commitment to ethical governance, operational excellence, and regulatory compliance.

Information Security Management Systems

Austrian Georgian Development LLC maintains an Information Security Management System (ISMS) designed to support the secure and resilient operation of its hydropower facilities. The ISMS is implemented in coordination with a trusted third-party IT and cybersecurity service provider and is tailored specifically to the risks and regulatory environment of the energy sector in Georgia.

The ISMS operated on the internationally recognized Plan-Do-Check-Act (PDCA) lifecycle, promoting continual improvement through structured planning, implementation, monitoring, and review. It incorporates not only IT security but also risks associated with operational technologies (OT), such as SCADA systems and field-level control, devices, which are integral to hydropower generation.

The ISMS includes the following core elements:

- **Asset identification and inventory,** covering both digital and physical assets. This includes IT equipment, operational systems, data repositories, field devices, and physical documents and equipment logs, all of which are inventoried and tracked to ensure protection based on their classification and criticality;
- **Risk analysis and evaluation**, aligned with the principles of ISO/IEC 27005[1], but adapted to the operational context of a small-to-medium-sized hydropower plant. Risks include cyber threats (e.g., malware, SCADA access attempts), physical risks (e.g., unauthorized entry, document loss), and third-party risks (e.g., vendor access to systems);
- **Threat modeling and risk treatment plans**, developed in consultation with IT specialists and based on realistic scenarios affecting power generation, data loss, or regulatory non-compliance. These plans prioritize controls that minimize operational disruption and data compromise;
- **Audit scheduling and follow-up,** including internal policy audits, technical system reviews, and alignment checks with applicable legal and lender requirements;
- **Continuous improvement and management review**, led by the Company General Director and the ESG Manager, with input from the IT service provider and technical advisor. Management reviews are held at least annually and involve examination of incident records, performance metrics, and upcoming regulatory changes.

Austrian Georgian Development LLC's ISMS reflects its core values of accountability, transparency and operational excellence. It not only meets the baseline security needs of its current operations but also provides a scalable framework for future growth, regulatory alignment, and cross-border compliance with international energy finance and ESG standards.

Cybersecurity Measures

Cybersecurity measures are a critical subset of Austrian Georgian Development LLC's broader information security strategy. They are specifically designed to prevent unauthorized access, misuse, or loss of personal,

[1] *ISO/IEC 27005 refers to the international standard that provides guidelines for information security risk management. It is part of the ISO/IEC 27000 family of standards, which focuses on information security management systems (ISMS).*

operational, and infrastructure-related data. Given AGD LLC's role as a hydropower plant operator and its reliance on digital and operational technology (OT) systems, cybersecurity protections extend across IT networks, cloud services, and SCADA environments.

The cybersecurity program is managed in coordination with a qualified third-party IT service provider and includes multi-layered safeguards that reflect both technical and administrative risk controls. These safeguards address common threat vectors such as malware, unauthorized remote access, and insider risks.

Key components of the company's cybersecurity framework include:

- **Regular use and active monitoring of antivirus and anti-malware software**, deployed across all corporate and operational devices. Updates are managed centrally and verified by the IT provider.
- **Enforcement of strong password policies and multi-factor authentication (MFA)** across remote access platforms, cloud-based tools, and administrative systems. All credentials are assigned based on role and are not reused across applications.
- **Controlled access systems** ensure that each employee and contractor uses unique credentials. Access rights are reviewed periodically and adjusted as roles change, or projects conclude.
- **Workstation security policies** include enforced password rotation, automatic screen locking, USB access restrictions, and endpoint monitoring for unusual activity.
- **Confidentiality protocols**, including clean desk policies and secure communication standards, are implemented across offices and field facilities. These measures ensure that sensitive paper documents, printed data, and mobile devices are not left unsecured.
- **SCADA systems are segregated from public networks. Access is granted only to a designated technical personnel, and such access is routinely audited**
- **Data backups** are performed regularly and stored in secure, encrypted cloud environments. Backup systems are tested periodically for reliability and recovery assurance.
- **Periodic reviews and testing** of security infrastructure are conducted to identify and resolve emerging threats. These assessments are part of the company's continuous improvement cycle and are scheduled at least once annually.
- **Cybersecurity performance and compliance reviews** are held periodically between AGD LLC and its IT provider. These include analysis of login activity, threat detection metrics, and response timeframes for any incidents or alerts.

Cybersecurity is not seen as a purely technical function but as an essential element of operational governance.

Through this integrated and proactive approach, AGD LLC ensures that its digital resilience keeps pace with evolving operational demands and cyber risk landscapes in the energy sector.

Data Protection and Legal Compliance

AGD LLC is fully committed to protecting personal and sensitive information in accordance with the Law of Georgia on Personal Data Protection and relevant international good practices. As an operator of hydropower infrastructure, AGD LLC processed personal data not only for internal employment and administrative needs but also in connection with site access, contractor management, compliance obligations, and stakeholder engagement.

The company ensures that personal data is handled with transparency, fairness, and purpose limitation. Data is collected only when necessary for business, operational, legal, or regulatory functions and is never used for purposes beyond those explicitly stated.

Core principles of Austrian Georgian Development LLC's data protection approach include:

- **Processing only the minimum personal data required** to fulfill business functions such as payroll, access authorization, contract administration, and legal reporting. Unnecessary or excessive data collection is explicitly prohibited.

- **Secure storage of all personnel, contractor, and third-party data**, whether in digital form or physical records. Storage systems are protected by encryption, physical access controls, and role-based digital permissions.
- **Clear access rights for data subjects**, including the ability to request information about how their data is used, to correct or update inaccurate data, and to request deletion or blocking of data where permitted by law. Requests are responded to within legally mandated timeframes and with appropriate documentation.
- **Retention of personal data only for the legally or operationally necessary period**, after which data is securely deleted, anonymized, or archived. Retention periods are determined by Georgian law, internal policy, and sector-specific requirements such as health and safety records, labor regulations, or environmental permits.
- **Secure disposal procedures** are enforced for both digital and paper-based records. Physical documents are destroyed using shredders. Digital files are securely erased using approved deletion software.
- **Vendor and contractor compliance** is a key part of AGD LLC's privacy program. Any third-party processing personal data on behalf of the company must sign contractual agreements that include specific data protection obligations. These include secure handling, data minimization, and cooperation in the event of an audit or incident.
- **Staff and contractors are regularly informed of their data rights** through induction training, and internal communication channels. AGD LLC emphasizes a culture of responsibility and awareness regarding the handling of sensitive information.
- **Video surveillance systems**, where deployed, are used solely for operational security and legal compliance. Signage is visibly placed, and footage is retained only for predefined periods unless subject to investigation.
- **Data breach notification procedures** are in place and reflect internationally recognized best practices. In the event of a suspected or confirmed breach involving personal data, the incident is escalated immediately to the IT provider. A formal investigation is conducted, and where necessary, data subjects and regulators are notified in accordance with legal requirements. Corrective and preventive actions are tracked and logged as part of the company's risk management process.

Training and awareness

AGD T LLC places strong emphasis on cultivating a security-aware culture across all levels of the organization. Every employee, from administrative staff to field technicians, is required to undergo structured training on information security, cybersecurity hygiene, personal data protection, and proper reporting procedures. This training ensures that personnel are aware of both the technical and ethical responsibilities associated with handling sensitive information and operating in a critical infrastructure environment.

New hires are required to complete a formal induction program prior to receiving system access or handling any operational data. As part of this onboarding process, individuals must review and acknowledge AGD LLC's Compliance Policy and Information Security Policy. This ensures a common baseline of understanding regarding the company's security standards, acceptable use of IT resources, and legal obligations under Georgian law.

Refresher training is delivered annually and updated as needed in response to legal or regulatory changes, security incidents, or internal policy revisions. All training sessions are documented and tracked for audit purposes.

Through its training and awareness program, AGD LLC reinforces individual accountability, reduces the likelihood of human error, and ensures that security and privacy obligations are understood and applied consistently across the organization and its partners.

Information Security Policy Annual Revision Process

Aligned with internationally recognized ESG practices and standards, AGD LLC undertakes a comprehensive review of its Information Security Policy at the end of each year. This systematic review, led by the Company ESG Manager, ensures that the policy accurately reflects current risk assessments, system performance metrics, and evolving operational practices. If any modifications are made during the revision process, the updated documentation is subjected to a thorough approval procedure. Initially, the proposed changes are carefully reviewed and endorsed by the Company General Director. Following this, the revised document is shared with the Caucasus Clean Energy Holding ESG and Sustainability Lead for final validation, ensuring that each modification adheres to the company's commitment to quality, transparency, and regulatory compliance. The Supervisory Board members are informed regarding any changes, reinforcing AGD LLC's commitment to maintaining high international ESG standards.

The updated version is uploaded onto the company's official website, while the previous version remains accessible in the archive folder to ensure transparency and continuity in governance documentation.