Protecting Your Information

About Vistra

Ranked among the top four corporate service providers globally, Vistra is a versatile group of professionals, providing a uniquely broad range of services and solutions. Our capabilities span across international incorporations to trust, fiduciary, private client services, and fund administration.

We employ over 4,000 professionals in over 80 cities across 46 jurisdictions throughout the Americas, Europe, Middle East, and Asia Pacific.

As a leading global player with expert industry knowledge and location specialists, Vistra has a deep understanding of the professional worlds of our clients, and a proven track record of offering highly versatile solutions, providing the people, processes, and products that help our clients get the most from their international business.

Introduction

Information is critical to all of our clients and is therefore a key priority for Vistra. We host hundreds of thousands of individual records worldwide. The security of this information is of the utmost importance and we continually make sizeable investments to protect our information, IT systems, applications, infrastructure and processes.

Digital networks are a key enabler in the expansion of our business. They dramatically enhance our ability to communicate, share and store information, and engage with colleagues and clients. New technologies bring new capabilities and, with new capabilities, an increased risk of uncontrolled data disclosure, modification or unavailability.

At Vistra, we believe that a strong business reputation depends on a robust information security and business resilience programme.

The purpose of this document is to summarise our approach to information security and business resilience. It provides an overview of how we secure client information and our systems housing this information, keeping in mind that the specifics of these measures may vary depending on the service and the applicable country regulatory requirements.

Our information security and business resilience programme and practices are focused on sharing information appropriately and lawfully, while providing confidentiality, integrity and availability.

SYSTEM CERTIFICATION ISO 27001 SGS

Our Approach to Information Security and Business Resilience

Vistra has developed and implemented a comprehensive information security and business resilience framework aligned to industry best practices such as ISO/IEC 27001:2013 the International Standard for Information Security Management System (ISMS), IT Infrastructure Library (ITIL) for IT Service Management, and ISO22301:2012 for Business Continuity Management Systems (BCMS).

We are ISO/IEC 27001:2013 certified for a number of our key sites. Our certificate is available to view on our website.

Vistra takes a multi-layered, defence-in-depth, approach to protecting the data Vistra has responsibility for; this includes physical, procedural, personnel and technical security to protect confidentiality, integrity and availability of information and services.

This framework and its underlying controls are designed to ensure that:

- Vistra information and systems are only available to authorised people with a justified business need;
- Vistra information is not disclosed or modified without authorisation;
- Vistra information is available when required by relevant business processes;
- Applicable regulatory, legislative and client requirements are met;
- Information security training and awareness is available for all workers;
- Breaches of security and suspected weaknesses are reported, investigated, documented and resolved;
- Workers have access to clear standards and guidelines that enabled the right attitudes and behaviours; and
- Our brand and financial resources are otherwise protected from the damage that information security breaches can cause.

Information Security and Business Resilience Governance and Policies

The Vistra Executive Committee (ExCo) provides top level commitment and support to information security and business resilience across the company which is demonstrated through a signed Information Security Mandate .

Information security and business resilience is overseen by the Vistra Information Security Group (VISG) that reports to ExCo. They oversee security projects, reports, objectives and key performance indicators. This group has representation from Vistra Information Technology, Human Resources, Compliance, Legal and our Divisions.

Vistra has a Baseline Information Security Policy and Standards Set that is aligned to ISO/IEC 27001:2013 and applied to all Vistra business units in all locations. They are owned by VISG and reviewed by key stakeholders across the business.

The Baseline Information Security Policy and Standards Set, and Business Continuity Policy is reviewed on an annual basis to reflect any significant changes in Vistra's structure, business functions and the regulatory environment; or in response to new and emerging threats.

The Baseline Information Security Policy and Standards Set is communicated to all workers through an information security training and awareness programme and is published via the dedicated information security section of Vistra's intranet.

Human Resource Security

All Vistra workers are subject to screening prior to employment. The screening processes are conducted in accordance with relevant national laws and industry regulations and provide verification of identity and credentials, as well as evaluating applicant integrity.

All Vistra workers are subject to confidentiality/non-disclosure agreements as part of the standard employment contracts and are required to comply with the controls outlined in the Baseline Information Security Policy and Standards Set, including an Acceptable Use Standard. All workers acknowledge that they can access and have read this documentation annually.

The VISG oversees the multi-lingual information security training and awareness programmes to ensure that all workers are aware of their responsibilities and possess the necessary resources to maintain our position on information security.

These programmes include mandatory annual online training for all workers; targeted security campaigns that are commensurate with specific issues such as simulated phishing exercises and more detailed technical security training for the Vistra technology teams such as secure software development.

When a worker leaves, Vistra applies robust procedures to ensure the timely removal of access rights to IT systems as well as the retrieval of any physical information assets which are recorded in the asset inventories.

Asset Management

Vistra has implemented an information classification scheme for all information that supports its day to day business activities. Vistra maintains inventories of its information assets, including applications and IT systems.

Vistra uses Enterprise Asset Management solutions to inventory our assets. The Acceptable Use Standard details the acceptable use by staff of those assets.

The Asset Classification and Handling Standard requires all client information to be classified and handled as CONFIDENTIAL.

Data Loss Prevention (DLP) software is deployed across the entire estate. All user endpoints by default DENY for removable media (e.g. USB, CD/DVD, mass storage devices).

Local certified companies are used for secure destruction for paper and magnetic media. The default destruction method for all assets containing information is physical destruction. Certificates of destruction are required and retained.

Physical and Environmental Security

All Vistra office locations operate risk-based controls to afford protection against unauthorised physical access. These can include physical and electronic access control systems, manned reception desks, CCTV and security lighting.

Access to our data centre facilities and other information processing locations is strictly controlled and restricted to pre-authorised individuals only. This access is logged and the access rights are reviewed on a regular basis.

All Vistra data centre facilities are rated Tier 3 or above, which provide a high level of redundancy, physical security and environmental control including fire detection and prevention, dual power supplies, monitored Uninterruptable Power Supply (UPS), back-up generators, temperature, smoke, water and humidity controls.

Access Control

Vistra operates on the principle of 'least privilege' for access control. This is to ensure that only authorised individuals are permitted access to our business applications, systems, networks and computing devices; that individual accountability is established and to provide authorised users with the access permissions that are sufficient to enable them to perform their duties but do not permit them to exceed their authority. Access is provided under Role Based Access Control (RBAC) and activity is logged and monitored.

Access is co-ordinated through the regional IT Support service desks and all access requests must be authorised by an employee's line manager and/or the assigned resource owner. There are regular reviews of user access rights to detect and remove any inactive accounts and inappropriate access permissions.

All Vistra employees are assigned unique user IDs and are required to select and manage their passwords in line with the Password Standard. In the event of a change of employment status or role, user access rights are immediately revoked or reassigned by the relevant regional IT Support service desk upon notification from the line manager.

The use of privileged accounts is strictly controlled and restricted to system administration and maintenance activities only. Additional measures are employed to securely manage these accounts. This includes enhanced password management controls such as more complex structure and increased change frequency.

Remote access to the Vistra network is only permitted for pre-authorised employees using a Vistra managed asset. This is achieved using an encrypted VPN solution and is supported by multi-factor authentication.

Cryptography

Vistra's Encryption Standard details the approved cryptographic algorithms and the process for encryption key management within Vistra. All Vistra desktops and laptops have full disk encryption using AES256. All backend mass storage is encrypted-at-rest using AES256. All backup tapes are encrypted using AES256. Exchanges of confidential information across untrusted networks are encrypted-in-transit using TLS or IPSEC.

Communications and Operations Security

Vistra has implemented a defence-in-depth approach to protect its information and IT systems from existing and emerging threats. The management and operation of our IT systems is delivered by our highly experienced technology teams using a service management model based upon the Information Technology Infrastructure Library (ITIL) standard. This includes the formalisation of processes and procedures to support core activities such as back-up and recovery, change management, release management and capacity planning.

Vistra has a resilient hub and spoke disaster tolerant network and computing architecture design across all of its global data centres. Where appropriate our multi-tier internet-facing infrastructure uses two physical layers of firewalls supporting three-tier application deployment and secure segregation of different networks, connections and systems. Server virtualisation provides rapid resource provisioning and enhanced failover and disaster recovery capabilities.

All Vistra IT systems are configured following technical security standards which include applicable controls such as system hardening, encryption, anti-virus and data loss prevention and regular patching. The VISG actively monitors security key performance indicators and works with the relevant teams to ensure that the current security controls deployed are both appropriate and effective, to mitigate risk.

The Vistra IT technical security controls are monitored by a security operations centre which collects and correlates the event logs from network devices, firewalls, IDS and web application firewalls. This data is analysed and any unusual or suspicious events generate the necessary alerts which are handled by our information security incident management processes.

System Acquisition, Development and Maintenance

Vistra follows a defined System Development Life Cycle (SDLC) that incorporates information security throughout each stage including risk assessments, the identification and implementation of control requirements, static and dynamic code analysis and technical security penetration testing.

Vistra maintains separate development, test and production environments and has strict policies to enforce segregation of duties for employees responsible for development, testing and support activities. Our source code, including all applications under development, are stored and protected in an approved source code system with audit logging enabled to track activity such as code modification and deletion.

Supplier Relationships

Vistra's supply chain assurance program covers third party activities which are audited based on risk for information security and business resilience. This may include the evaluation of prospective vendors for compliance with Vistra's ISO27001/2 aligned Baseline Policy and Standards Set , risk identification, rating and finding management, contract review including confidentiality clauses, the right to audit and detailed contractual security requirements where required.

Information Security Incident Management

Vistra has global risk-based processes to respond to information security incidents, unusual or suspicious events and breaches of policies. These processes are owned and coordinated by the Information Security Team with formal involvement from relevant stakeholders (e.g. legal, compliance, technology, human resources, business relations and anti-fraud, marketing and public relations).

The information security incident management processes are designed to contain and control the incident, reduce any potential impact to the business, identify and investigate the root cause and implement corrective actions to reduce the risk of recurrence. These processes are supported by procedures for identification, reporting, assessment, response, recovery and follow-up. Our post-incident procedures include root cause analysis, forensic investigation and, where required, notification to the relevant authorities and affected clients.

All Vistra employees are provided with training and guidance to identify and report information security incidents.

Business Continuity Management

Vistra has an established Business Continuity Management programme that supports our regulatory and contractual requirements.

Our programme is managed by dedicated office business continuity coordinators and is underpinned by relevant business continuity policies, procedures and supporting technologies.

All Vistra business units are included within the business continuity management programme and are required to have in place a business continuity plan. Our business continuity plans and disaster recovery plans are developed and maintained by assigned owners from within the business units and information technology teams and are regularly updated to reflect any change of circumstances.

Vistra performs business continuity and disaster recovery tests on a periodic basis to ensure that the plans can be employed should the need arise.

Audit and Compliance

The VISG oversees and measures compliance with the Information Security Policy and Standards through periodic technical and non-technical control assessments. Our technical control assessments includes quarterly vulnerability scans and annual penetration tests using United Kingdom National Cyber Security Centre CHECK approved testers. Our non-technical control assessments include internal audit, information security management system reviews and security KRIs.

We are externally audited yearly to maintain our ISO/IEC 27001:2013 certification. Our certficate can be viewed on our website.

The results of these reviews are documented, managed through to remediation and reported to VISG on a monthly basis.

Our Security Delivery Model

Our security delivery model is focused on four workstreams:

- Defend and Prevent
- Hunt and Detect
- Respond and Recover
- Governance

Defend and Prevent

Ensure that the Vistra staff, policies, processes, practices, and technologies proactively defend Vistra from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with Vistra risk appetite.

Internal Information Security Audit – audit business units against the Information Security Baseline Policy and Standards Set and support business units in their compliance to the Policy and Standards. Track to closure or acceptance of any mitigation advice.

Secure Projects & Programmes – support the business with security advice from project conception to service decommission. Ensure the new information based services are 'secure by design', secure throughout their life and securely decommissioned at end of life.

Secure Supply Chain – on boarding due diligence and from therein ongoing audit, ensure that our suppliers are equal to or exceed our information security standards. Where they do not, the risk is remediated or the business is aware of what risks they are accepting.

Secure Culture – on top of the minimum group training, deliver awareness campaigns on key issues and policy requirements, including news articles, posters, leaflets, lunch and learns, onsite briefings to staff and management. Bring security to life.

Mergers & Acquisitions – support any due diligence on potential acquisitions, understand their information security posture, support the acquisition on migration to Vistra information security policy and standards.

Business Support & Advice – act as a centre of expertise and excellence on information security, be known and approachable by all stakeholders of the business.

Hunt and Detect

Ensure that the Vistra staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries, and manage instances of suspicious and unauthorised events as expeditiously as possible.

External Penetration Testing & Vulnerability Scanning – coordinate external specialists on penetration testing, working with internal stakeholders on remediation and escalate where there are challenges.

Internal Vulnerability Scanning – undertake internal vulnerability scanning across all our infrastructure hunting for vulnerabilities and weakness that can be remediated. Work with stakeholders on immediate remediation on strategic solutions to common vulnerabilities.

Protective Monitoring – deploy and operate an SIEM solution to centralise logging information and monitor and investigate events based on clearly defined use cases.

Incident Response – provide technical incident response capability, basic forensics, investigation and support as a technical SME to line management, HR, legal, compliance and law enforcement as required.

Threat Intelligence – monitor threat sources (open source & privileged source) on emerging threats and attacks, provide advice to technical stakeholders on immediate action where necessary.

Technical Exercising – undertake wider social engineering testing and exercising, including phishing attacks and supporting the Respond & Recover activities where required.

Respond and Recover

When an incident occurs, minimise its impact and ensure that Vistra staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible. Assets include technologies, information, people, facilities, and supply chain.

Business Continuity Strategy – undertake or support the business in undertaking Risk Assessments and Business Impact Assessment in order to determine appropriate Business Continuity Strategies.

Business Continuity (BC) Planning – develop, consult, publish and provide support to the BC coordinator network on business continuity templates, tools, group wide services and other resources to support them in the BC activities.

Crisis Management/Emergency Planning – support the Vistra leadership team and office management teams in putting in place crisis and emergency planning for that first 'golden hour' of an incident.

Training & Awareness – train the BC Coordinator network on the tools/templates and services available to support them in the BC activities. Promote our BC practices both internally and to our clients/regulators/interested parties.

Validation/Testing/Exercising – standardise test reporting, provide oversight and reporting on that reporting across the group. Working with the Hunt & Detect service to undertake desktop/table top exercising and tests.

Group Solutions – evaluate, select and operate group technical solutions to support BC planning, testing and invocation (e.g. call Cascade solutions). Achieve, maintain and expand ISO22301 where it has value. Support the business in understanding and selling this certification in there every day conversations with existing or potential clients.

Governance

Ensure that the Vistra leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all information security and business resilience activities. This function includes ensuring compliance with all external (client/regulator) and internal requirements and mitigating risk commensurate with the organisation's risk appetite.

Strategy, Objectives and Business Integration – ensure the teams activity has top level buy in and support, all activity is aligned to business objectives and integrated in to wider functional areas such as Compliance, Human Resources, Legal and Information Technology.

Policy & Standards – ensure clear, organisationally aligned and integrated policy and standards are in place that meet legislation, regulator & client requirements and organisational risk appetite.

Internal & External Relations – provide confidence to internal and external stakeholders that there are adequate and effective controls in place. Respond to requests for client proposals, regulatory audits and internal questions, selling our internal services.

Reporting & Performance Measurement – develop Key Risk Indicators (KRIs) to measure the effectiveness of information security controls to facilitate decision making, increased performance and increase accountability through this measurement. Report to key stakeholders on key information security activities, known risks and non-conformities, and evaluation against KRIs.

ISO27001 Certification – achieve, maintain and expand ISO27001 where it has value. Support the business in understanding and selling this certification in there every day conversations with existing or potential clients.

Priorities & Resourcing – determine current and future priorities and resources needed to meet objectives. Collaborate with internal and external stakeholders to find efficiencies.

Summary

Clients and individuals rightfully demand accountability from any organisation handling their personal and confidential data. We understand the importance of taking appropriate steps to safeguard information and are committed to protecting information relating to our clients and to our people.

We trust this demonstrates the commitment and considerable investment Vistra has made to information security and that our clients, business partners, employees and investors/shareholders can have full confidence in the confidentiality, integrity and availability of our information and IT systems.

If you have any specific questions or would like additional information on the measures that we take to protect your information, then please contact your nominated Vistra relationship manager.