



# Protecting Your Information

January 2026



**Disclaimer**

This document is subject to and must be read in conjunction with our legal Notice (including Disclaimer) [www.vistra.com/notices](http://www.vistra.com/notices).  
Copyright ©2026 by VistraGroupHoldings SA. All Rights Reserved

<b>Section</b>	<b>Page</b>
Introduction	2
Our Approach to Information Security and Business Resilience	2
Information Security and Business Resilience Governance and Policies	3
Human Resource Security	3
Asset Management	4
Physical and Environmental Security	4
Access Control	4
Cryptography	5
Communications and Operations	5
System Acquisition, Development and Maintenance	5
Supplier Relationships	6
Information Security Incident Management	6
Business Continuity Management	6
Audit and Compliance	7
Summary	7

# 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-specific 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.

## 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 27001:2022 the International Standard for Information Security Management System (ISMS), IT Infrastructure Library (ITIL) for IT Service Management, NIST Cybersecurity Framework 2.0 and ISO22301:2012 for Business Continuity Management Systems (BCMS).

We are ISO/IEC 27001:2022 certified for the majority 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; these 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 colleagues.
- Breaches of security and suspected weaknesses are reported, investigated, documented and resolved.
- Colleagues 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 an 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 risk and performance indicators. This group has representation from Vistra Information Technology, Human Resources, Compliance, Legal and other essential departments.

Vistra has a Baseline Information Security Policy and Standards Set that is aligned to ISO/IEC 27001:2022 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 colleagues 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 colleagues 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 colleagues are subject to confidentiality/non-disclosure agreements as part of the standard employment contracts and are required to comply with Vistra's Information Security Policy and Standards. All colleagues acknowledge that they can access and have read these documents annually.

The VISG oversees the multi-lingual information security training and awareness program to ensure that all colleagues 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 colleagues; 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 colleague 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 Policy details the acceptable use of those assets by colleagues.

The Data Classification Scheme and Handling Guidelines 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 colleagues 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) systems, 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 colleagues are permitted access to our business applications, systems, networks and computing devices; that colleague 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 coordinated through the regional IT Support servicedesks, and all access requests must be authorised by a colleague'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 colleagues 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. These 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 colleagues using a Vistra managed assets. This is achieved using an encrypted VPN solution and is supported by multifactor 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 modern TLS or IPSEC.

# Communications and Operations

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. These 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 Secure System Development Life Cycle (SSDLC) that incorporates information security throughout each stage including security by design, 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 colleagues 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 employs a risk-based approach to managing its supply chain assurance program. These includes evaluating prospective vendors for compliance with global data protection frameworks and Vistra's ISO27001/2 aligned Baseline Policies and Standards Set, identifying and rating risks, managing findings, and reviewing contracts - including confidentiality clauses, the right to audit and detailed contractual security requirements wherever required.

Vistra monitors critical third parties using recognised external risk-rating services and other continuous-assurance mechanisms.

Vistra also evaluates the presence of sub-processors and fourth-party dependencies to ensure the extended supply chain meets our security expectations.

# 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 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, wherever required, notification to the relevant authorities and affected clients.

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

Vistra assesses historical security incidents and evaluates each supplier's ability to respond, remediate and communicate effectively.

# Business Continuity Management

Vistra has an established Business Continuity Management programme that supports organisational resilience and 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 a business continuity plan in place. Our business continuity 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.

Vistra takes a rigorous, defence-in-depth approach to security testing and assurance. All penetration testing is performed by certified testers using CREST rules of engagement as standard, and the majority of our estate including cloud platforms, networks, firewalls, and external attack surface is under continuous monitoring. We conduct authenticated tests on all client-facing applications and a global black-box penetration test to provide a comprehensive, real-world view of our security posture.

In addition to that Vistra performs control assessments including internal audit, information security management system reviews and security KRIs.

We maintain our ISO/IEC 27001:2022 certification through annual external audits. Our certificate 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.

## Summary

Clients and colleagues 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 in information security and that our clients, business partners, colleagues 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.