# Information and Network Security

## Customer Reference Guide

May 2025
Version 1.0

**Disclaimer**

This document is provided as summary information only. It is not a contract, and no statement, representation, or characterization within this document shall be construed as an implied or express commitment, obligation, or warranty on the part of Inc. or any of its affiliates, or any other person.

All contractual obligations between and its Customer are set out exclusively in a written agreement with the Customer, and nothing in this document shall amend, modify, supplement or otherwise change the provisions or terms of that agreement.

LevelBlue may, in its sole discretion, alter the policies and procedures described in this document without notice to or consultation with any Customer or another person. Customers are responsible for maintaining security policies and programs appropriate to their enterprises.

# Table of Contents

# To the Reader

This document is designed for the use of LevelBlue (“LevelBlue” or “Company”) current and potential business customers (“Business Customers” or “Customer”). The document provides:

- An introduction to LevelBlue and its global security organization
- A review of LevelBlue security roles and responsibilities
- A summary of Customers’ security responsibilities

An overview of LevelBlue security policy and comprehensive programs that strive to incorporate security into every facet of LevelBlue computing and networking environments.

This overview focuses on the key elements and initiatives to safeguard LevelBlue Customers and their data while managed by LevelBlue or in transit on a LevelBlue network. In general, the use of ‘security’ throughout this document refers to information and network security.

For further information regarding LevelBlue, visit our website at levelblue.com or contact your local LevelBlue account team.

# Introduction to LevelBlue

## 1. About LevelBlue

LevelBlue (formerly AT&T Cybersecurity) is a managed security service provider that simplifies cybersecurity through its award-winning services, experienced, strategic consulting, threat intelligence and renowned research. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow.

## Products

LevelBlue serves as a trusted advisor to manage risk while businesses innovate with confidence. LevelBlue services include:

Cybersecurity Consulting Services provide ongoing assessment, planning and advisory through the LevelBlue Consulting team, which has an average of 15-years experience in cybersecurity. Organizations realize business transformation with LevelBlue Consulting services that sharpen security strategy and build cyber resilience through Zero Trust, risk mitigation, and compliance assurance.

Managed Security Services for Network Security, Threat Detection and Response, and Endpoint Security offer a strategic extension to help organizations simplify cybersecurity to deliver greater insights. LevelBlue Managed Security Services drive efficiency in security operations, identify costs and complexity and associate them with business outcomes, and pinpoint where to adapt and scale as business evolves.

Threat Intelligence from LevelBlue Labs helps proactively identify threats and accelerate threat detection and response through its threat intelligence platform. Enriched by machine learning and security expertise, the platform is backed by the LevelBlue Open Threat Exchange (OTX), a community of over 235,000 security professionals who submit 20 million plus threat indicators daily—so customers can effectively prepare for a potential data breach.

Additionally, LevelBlue offers powerful, third-party integrations through its open XDR platform USM Anywhere.

LevelBlue operates across four global Security Operations Centers (SOCs) and three global Network Operations Centers (NOCs) that are always on and monitored 24/7/365, providing continual service and support.

## 2. LevelBlue Labs

LevelBlue Labs is the Threat Intelligence Unit of LevelBlue. With an unrivaled vantage point of the Threat Landscape, LevelBlue Labs Threat Intelligence makes it easier for our customers to quickly identify, assess, and respond to threats.

Our research team delivers tactical threat intelligence that powers resilient threat detection and response—even as your IT systems evolve, and adversaries change their tactics, techniques, and procedures (TTPs).

LevelBlue Labs includes a global team of threat researchers and data scientists who, combined with proprietary technology in analytics and machine learning (ML), analyze one of the largest and most diverse collections of threat data in the world.

# Security Operations

LevelBlue employs a bespoke security operations framework designed to provide continuous, proactive protection for organizational data, systems, and business processes, and those of our customers. Our aim is to do more than simply react to threats, but to anticipate them before they occur.

At its core, our approach blends security best practices, compliance controls, real-time threat monitoring with advanced incident response capabilities. We maintain a 24/7 Security Operations Center (SOC) to identify, track, and mitigate technical risks before they can impact operations.

In addition to reactive measures, our Security Operations include proactive strategies such as vulnerability management, continuous control testing, and periodic security assessments. Our security teams work hand-in-hand with our compliance and audit teams to ensure that every layer of protection is actively tested, continuously improved, and aligned with industry standards.

## The Mission

Our mission is simple, but vital: **To safeguard trust by securing the systems and data that power modern business.** We believe that security is more than an obligation or a box to be checked—it is a vital component to building a successful business, and a shared commitment between ourselves and our customers. By focusing on integrity, transparency, and continuous improvement, we strive to create a strong program that meets or exceeds the highest standard of security across every aspect of our operations.

At LevelBlue, we truly believe that security is a journey, not a destination. Our mission drives us to stay ahead of emerging threats and continuously evolve our approach. We understand that trust is earned, and our goal is to be a trusted partner in our customers' journey to secure their digital assets, meet their compliance or security controls, and improve their own operations.

Through our mission, we aim to be more than just a managed security service provider. We want to be a security **partner** that **empowers** our customers to pursue innovation and growth without compromising on protection. Our mission guides every decision, from the technology we deploy to the people we hire and the processes we create.

## The Process

Our process encompasses four key areas that follow a clear, structured methodology designed to reduce risk and enhance protection at every layer. Our approach is cyclical and covers:

**Assess:** We start with comprehensive risk assessments, threat modeling, and vulnerability scans. By identifying specific risks to our environment, we create a targeted security roadmap tailored to our unique needs.

**Implement:** Based on the results from the assessments, we identify and implement multi-layered security controls to provide a comprehensive response to risks or vulnerabilities.

**Monitor:** Our 24/7 SOC constantly monitors for threats using real-time analytics, assisted by an industry leading open threat exchange and machine learning. Alerts are analyzed by trained, certified security experts who leverage their extensive experience to provide timely guidance on mitigation, remediation, and incident management.

**Improve:** Security is a living process. As technologies change, organization grows, and needs shift, new security controls may be required. By conducting regular audits, penetrating tests, and other technical control testing, LevelBlue strives to continuously improve and mature our operations and security. Insights from these activities are used to update every aspect of our security operations, including policies, technology stack, and incident response playbooks.

## The Layers

To fully meet the complex requirements of modern cybersecurity programs, LevelBlue has created a multi-layered process that supports and defines our security operations. These have been broken out into the following four layers:

**Best in Class Security Operations:** At the edge of LevelBlue security program stands our best-in-class security operations. This comprises our real-time monitoring programs, layered security controls, and comprehensive framework management. LevelBlue regularly invests in technology to ensure the organization stays secure and can meet the high expectations of both ourselves, and our customers.

**Strong Organizational Compliance:** Like security itself, compliance is a means to further add value and improve our business and operations, rather than a simple box to be checked. Maintaining compliance with regulations, laws, contractual requirements, and industry frameworks is a fundamental piece of LevelBlue security program.

**Strategic Control Testing:** All deployed security controls undergo regular testing following defined strategies, organizational needs, and in line with industry expectations. Testing, as with all our processes, is multi-layered, and includes continuous automatic monitoring, targeted manual tests, external reviews, and more.

**Security First Culture:** This is the bedrock on which everything else is built. At LevelBlue every employee is considered a key component in ensuring security is successful. We continuously invest in our employees' training, ensuring that they have a strong understanding of not only the value of security, but also their role in ensuring its success.


Figure 1: LevelBlue Security Operations Visualized

# The Chief Security Office

The Chief Security Office (CSO) comprises several teams and serves as the tip of the spear responsible for driving security throughout the entire organization. The CSO develops the strategy for the enterprise, along with ensuring the tactical and operational aspects of security are met, including identifying risks, implementing, enforcing, and auditing security controls.

## Security Awareness and Education Programs

The Chief Security Office is charged with managing the security awareness program across the enterprise. The program comprises targeted security awareness initiatives promoted internally within, an internal awareness newsletter, all-employee bulletins and communications, and employee security awareness exercises. The CSO also maintains and updates the security training curriculum and provides an annual Security Awareness Corporate Compliance course. The Compliance course trains against the major cybersecurity tenets. All corporate employees and contractors are required to take this course. The CSO tracks completions of the Compliance course in conjunction with the corporate training organization.

In addition, all personnel are required to annually acknowledge their responsibilities to adhere to the Code of Business Conduct, information security policy, and information protection requirements.

## Security Policy and Documentation

It is the policy of LevelBlue to protect our information, infrastructure, and services, (“Information resources”), in all their forms from unauthorized or improper use, theft, accidental or unauthorized modification, disclosure, transfer, or destruction. This is achieved through the analysis of security risks to create security requirements that address those risks commensurate with the information resources’ sensitivity, value, and criticality.

This policy applies to all Information resources which are created, used, or maintained by or on behalf of LevelBlue or its customers unless superseded by a customer contract.

In protecting Information resources, it is our obligation to comply with all applicable laws and government regulations, including those that relate to the safeguarding of personal information and critical infrastructure.

The Chief Security Office develops, maintains, and issues specific security requirements and other reference materials in support of this policy. The security standards and reference materials comprise the Security Policy and Standards content, which is the basis for all security controls that protect Information resources. LevelBlue Security Policies and Standards are not shared externally except when approved, necessary, and under strictly controlled circumstances with proper non-disclosure agreements in place.

## Security Control Selection, Implementation, Testing, and Maintenance

Effective security depends on the selection, implementation, testing, and maintenance of robust controls that are tailored to the unique needs of our organization and our clients. Our processes begin with identifying specific threats, vulnerabilities, and compliance requirements. From there we select individual controls, or entire frameworks, to lay out our administrative, technical, physical, and operational activities.

During the implementation of internal controls, the CSO works with stakeholders across the organization to seamlessly integrate defined requirements into day-to-day operations. The team ensures each control is correctly configured and aligns with organizational policies and technologies. This phase also includes rigorous documentation to support future audits, maintenance, and compliance efforts.

While all controls and changes are reviewed and validated prior to implementation to ensure they do not negatively impact the organization's security or operations, testing does not stop there. Once implemented, controls are added to LevelBlue's extensive testing processes, and undergo various reviews including vulnerability scans, penetration testing, and similar alongside other systems.

Beyond this, maintenance is an ongoing effort across the entire enterprise. Security controls are regularly reviewed and updated to keep pace with evolving threats, technological advancements, and organizational needs. This includes patch management, change management controls, organizational training, and similar. By combining these efforts, we ensure that security controls remain effective, resilient, and adaptable, providing lasting protection and peace of mind.

Lastly, in order to ensure LevelBlue's security controls are properly implemented and documented, they are all tied back to industry standard security frameworks. Although internal auditing is conducted on a regular basis, LevelBlue has audits conducted by 3rd parties to confirm compliance.

# Personnel Security

LevelBlue is committed to maintaining a safe and secure workplace for its employees, Customers, and assets. To support this commitment, comprehensive background screenings are conducted for all candidates—including rehires—globally after an offer of employment is extended. Employment is contingent upon the successful completion of this screening process. Background checks may also be conducted for current employees transitioning into sensitive roles, in support of Customer requirements, or as required by applicable law.

Standard background checks typically include criminal history, identity verification, employment and education verification, sanctions checks, and professional reference checks, with variations depending on local legal requirements. Additional checks may be required for roles involving sensitive information, financial responsibilities, or government contracts. All screenings comply with applicable laws, including FCRA and GDPR. Candidate consent is obtained, and data is handled securely.

# Contractor Security

LevelBlue ensures that all contractors—including AT&T employees supporting LevelBlue—undergo appropriate background screening by their employers and are informed of their responsibilities regarding LevelBlue and Customer assets, in alignment with the LevelBlue Code of Business Conduct.