TaskUs™

CYBER SECURITY POLICY

PROJECT INTRODUCTION

TaskUs is dedicated to protecting data, privacy, and operations. We have refined our cybersecurity framework to incorporate best practices, align with global regulations, and emphasize continuous improvement, ensuring data integrity, confidentiality, and availability.

WHAT ARE WE PROTECTING

Computer Hardware

- Includes CPUs, disks, emails, web and application servers, PCs, and associated systems.

System Software

- Operating systems, database management systems, backup and restore software, and communication protocols.

Communication Network Hardware and Software

- Comprising routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management tools.

Application Software

- Both custom-written applications and commercial off-the-shelf software used by various departments.

THREATS TO SECURITY

TaskUs recognizes that cybersecurity threats can arise from both internal and external sources. Effective mitigation strategies require understanding the following primary threats:

EMPLOYEES

Employees pose a significant security risk, whether through negligence or malicious intent.

AMATEUR HACKERS AND VANDALS.

These attackers exploit vulnerabilities for opportunistic crimes, such as planting malware or misusing system resources.

CRIMINAL HACKERS AND SABOTEURS.

These skilled attackers may target TaskUs to access sensitive data or disrupt operations. While the likelihood of such an attack is lower, the impact can be severe.

KEY COMPONETS

CURRENT EMPLOYEE TRAINING AND AWARENESS

TaskUs prioritizes employee training to ensure security awareness, starting with New Employee Orientation (NEO) focused on data protection. Employees receive ongoing training via an LMS, intranet resources, and regular security updates. Annual security training is mandatory, with specialized programs for IT teams. Phishing simulations are conducted regularly, and DMARC policies are in place to prevent email spoofing and phishing risks.

EMPLOYEE TRAINING AND AWARENESS ENHANCEMENTS

- Gamified Learning Modules
- Weekly Micro-Learning Sessions
- Semi-Annual Workshops
- AI-Based Email Threat Detection Tools

CURRENT VENDOR MANAGEMENT & BACKGROUND CHECKS

TaskUs ensures rigorous background checks for new employees and contractors, including identity, education, work history, and criminal record verification. Third-party vendors with access to sensitive data are also thoroughly evaluated through security questionnaires and risk assessments. TaskUs is an active member of the Vendor Security Alliance, promoting Internet security via standardized assessments.

VENDOR MANAGEMENT & BACKGROUND CHECKS ENHANCEMENTS

Ongoing employee re-screening for high-risk roles

Periodic Vendor Audits

Annual external reviews of vendor management

CURRENT PHYSICAL SECURITY

TaskUs employs a comprehensive physical security model at their contact centers, including CCTV monitoring, security guards, and ID badge access for employees. Biometric systems and motion sensors enhance access control, and visitors are always escorted. Mobile devices are restricted, and server rooms have stringent security measures such as biometric access, fire suppression, smoke detectors, and backup power systems. This multilayered approach ensures the security of their facilities.

PHYSICAL SECURITY ENHANCEMENTS

AI-Powered CCTV Analytics

Periodic Access Log Reviews

RFID Technology for Equipment Tracking

Routine Server Room Audits

CURRENT NETWORK SECURITY

TaskUs uses a layered network security model with next-generation firewalls, VLAN segmentation, and micro-segmentation to safeguard systems and partner data. Tools like PAN Threat Prevention, URL filtering, and data filtering protect against threats and unauthorized data transfer. Regular reviews and strict change management ensure ongoing security and system integrity.

NETWORK SECURITY ENHANCEMENTS

Zero Trust Network Access

Regular Penetration Testing

TOOLS

TOOLS

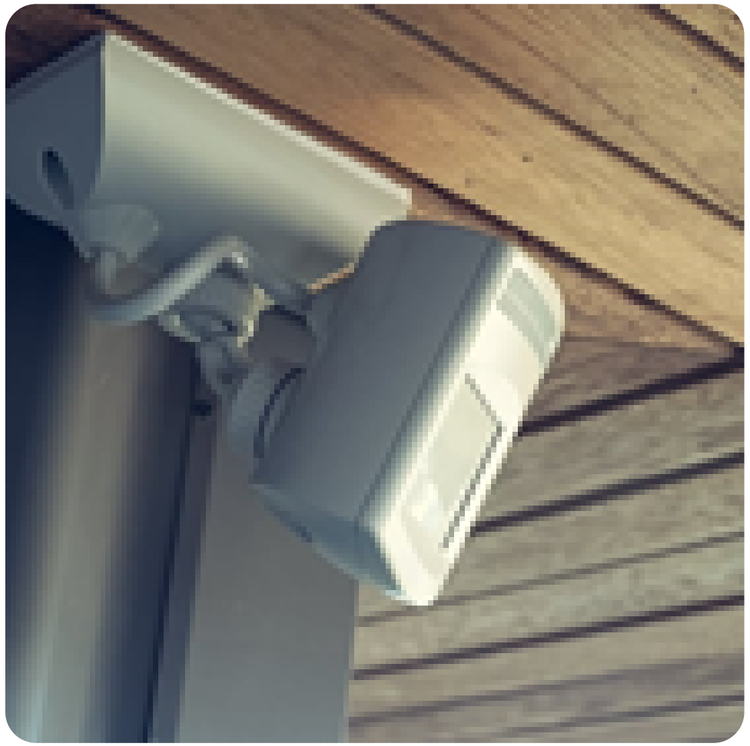
CCTV

Facial Image Recognition

Fingerprint Scanners

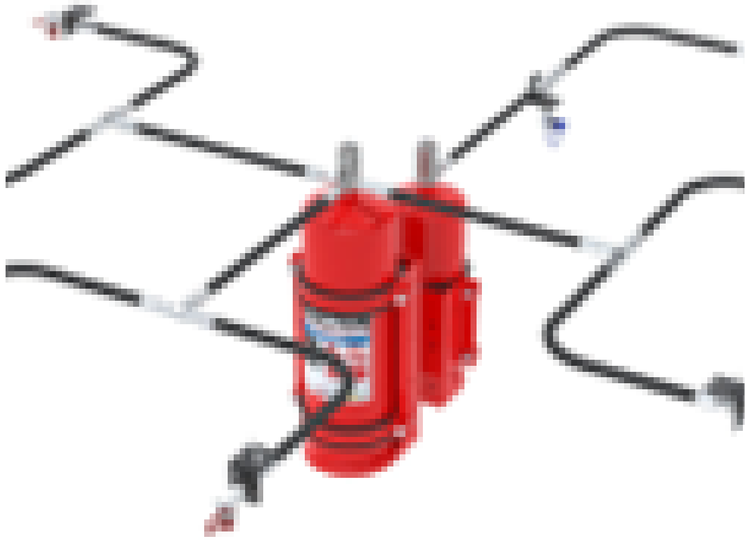
TOOLS

Motion Detector



**Biometric-
Restricted Access Control**

Fire Suppressor



TOOLS

Smoke Detector

Backup Power Generator

TOOLS

(PAN) Next Generation Firewalls

Palo Alto Firewall

Firewall Firm
MANAGED FIREWALL SOLUTION PROVIDER

Skyhigh Cloud Access Security Broker

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

TOOLS

Google Mobile Device Management

Bitium Identity as a Service (IdaaS)

BITIUM

Antivirus Software

TOOLS

Full Disk Encryption

Host Data Loss Prevention (DLP)

System File Integrity Monitoring (FIM)

ACCESS CONTROLS

ACCESS CONTROLS OVERVIEW

TaskUs manages user accounts with centralized access controls, assigning unique IDs and applying the principle of least privilege. Password policies and account security are enforced through Active Directory, with mandatory two-factor authentication (2FA) for remote and privileged accounts. Bitium IdaaS is used for identity management and cloud access, ensuring secure account provisioning. Regular account reconciliations and access reviews align user rights with job responsibilities.

ACCESS CONTROLS

NORMAL USER IDENTIFICATION

All users are required to have a unique login ID and password for access to TaskUs systems. The confidentiality of passwords is paramount. Users must adhere to the following guidelines regarding password creation and maintenance:

- Passwords must not consist of easily guessable information
- Passwords must not be written down or displayed near computer terminals to prevent unauthorized access
- Passwords must be changed every 90 days.
- User accounts will be frozen after 5 failed login attempts.
- Logon IDs and passwords will be suspended after 90 days of inactivity.

ACCESS CONTROLS

SYSTEM ADMINISTRATOR ACCESS

System Administrators, network administrators, and security administrators will have appropriate access to host systems, routers, hubs, and firewalls as necessary to fulfill their job responsibilities.

All system administrator passwords will be deleted immediately upon the termination or departure of any employee with access to those passwords.

ACCESS CONTROLS

SPECIAL ACCESS

Special access accounts are available for individuals requiring temporary system administrator privileges to perform their job duties. These accounts are monitored by the company and require prior approval from the user's IT Manager. Monitoring is conducted by maintaining a record of users with special access, and periodic reports will be generated for management review. Reports will detail who currently has special access, the reason for access, and the expiration date.

Special access accounts will expire in 30 days and will not be automatically renewed without written permission from management.

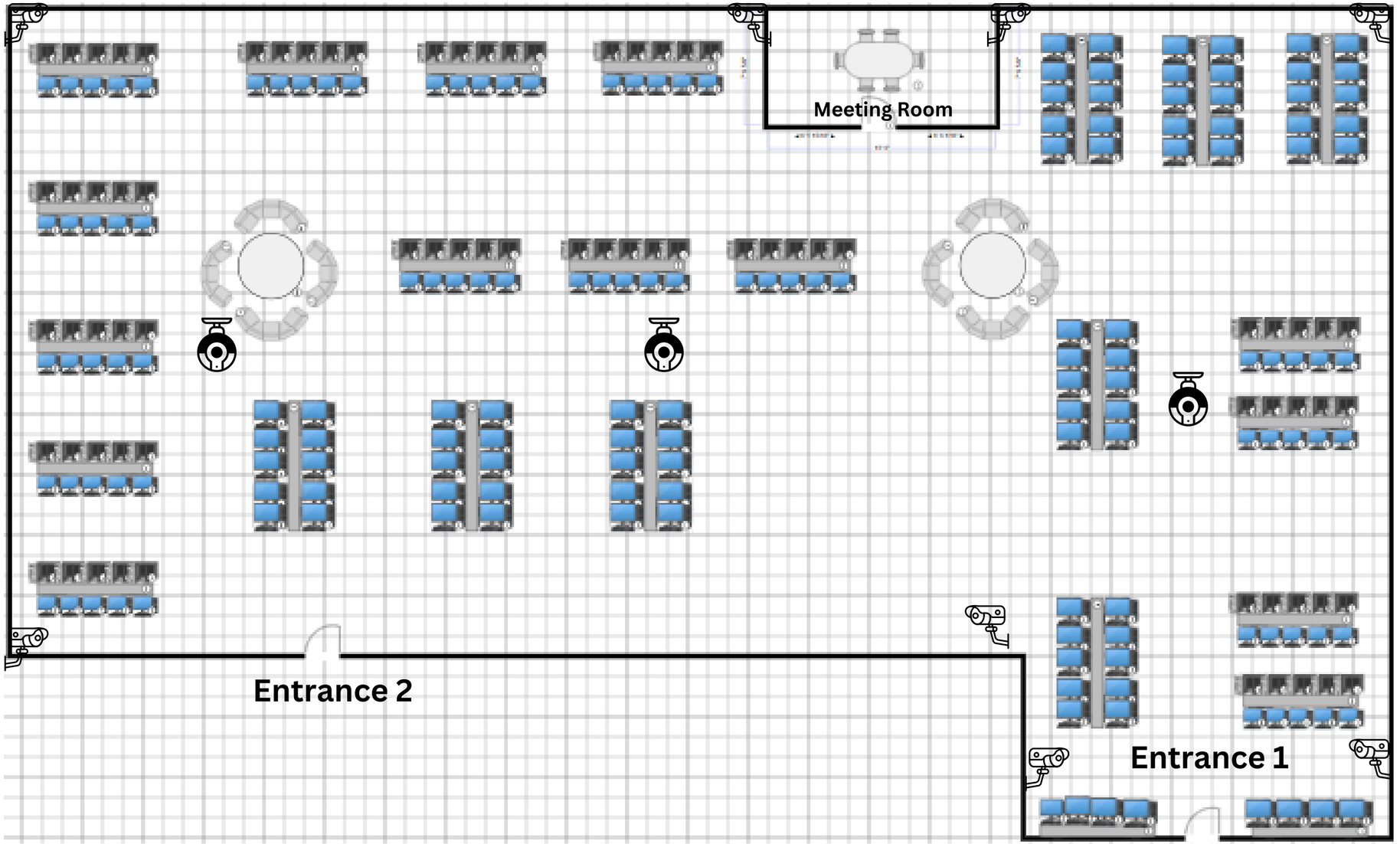
INCIDENT RESPONSE

INCIDENT RESPONSE

TaskUs follows a strict incident management process to address security events that threaten system and data integrity. Incidents are logged, prioritized by severity, and handled based on their impact on partners. The Incident Response Plan outlines seven stages: preparation, identification, containment, eradication, recovery, breach notification, and after-incident review. In case of a data breach, TaskUs quickly notifies affected partners and assesses the breach's scope. The plan is regularly tested to ensure efficient and timely incident resolution.

TaskUs Incident Response Process

Main Production Office



THANK YOU