WHITEPAPER

Bluedrop's Approach to Security

Summary

Bluedrop ISM offers a multi-layered security program dedicated to ensuring our customers have full confidence in our custodianship of their critical data.

Contact

For more information, please contact: isc@bluedrop.com or visit our website at www.bluedrop.com

Bluedrop ISM

Introduction

Bluedrop ISM (Bluedrop) is a globally recognized technology innovator that transforms training delivery and credential management for workforces that stretch across many employers. Our training management solutions help employers and workers threatened by a fast-changing labour market to survive and thrive.

In doing so, we are steadfast in our commitment to securing the data of our customers and their customers, who are the training providers, employers, workers, and other solution end-users. Data security and user privacy are amongst our most important responsibilities. Bluedrop is therefore committed to being fully transparent about our security practices and to helping our customers understand our approach.

About SkillsPass

Our flagship SkillsPass ISM platform provides true Integrated Skills Management (ISM) across industries, jurisdictions, and training requirements that would overwhelm a traditional Learning Management Solution (LMS).

SkillsPass is leveraged by governments and crossborder industry groups around the globe to advance critical skill development and credential management for the benefit of employers and their workers. Today, close to 3 million global worker records are securely stored on SkillsPass.

For more information or to schedule a demo of SkillsPass, simply visit us.

Organizational Security

Bluedrop has established a security program dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our security program is aligned with the SOC 2 Type 2 and PCI Compliance standards and is regularly audited and assessed by third parties.

Our commitment to security and compliance flows throughout every facet of the Bluedrop ISM organization. The solutions we provide are battle-tested and have met the highest levels of audit scrutiny related to data security, privacy/consent legislation, and web content accessibility guidelines.

1 Personnel Security

Bluedrop's personnel practices apply to all members of the Bluedrop workforce, including regular employees and contractors who have direct access to Bluedrop's internal information systems. All employees are required to understand and follow internal policies and standards. Before gaining initial access to systems, all employees must agree to confidentiality terms and take security training. Upon termination of work at Bluedrop, all access to Bluedrop systems is removed immediately.

2 Security Training

During their tenure, all employees are required to complete security training. They are also required to acknowledge that they've read and will follow Bluedrop's information security policies. Some employees, such as software developers, operators and support personnel have elevated access to systems or data.

“

As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.”

Newton Lee

3 Divide & Conquer Approach

Our holistic approach to security permeates the organization, with each division and operating unit understanding their roles and responsibilities within the security program. For example:

Software Product Development

- Establish secure development practices and standards
- Ensure project-level security risk assessments
- Provide design review and code review security services for detection and removal of common security issues
- Train developers on secure coding practices

Compliance

- Coordinate regular risk assessments, and define and track risk treatment
- Coordinate audits and maintain security certifications
- Respond to customer inquiries
- Review and qualify vendors for compliance

Operations & Information Security Team

- Build and operate security-critical infrastructure including Bluedrop's public key infrastructure, event monitoring, and authentication services
- Maintain a secure archive of security-relevant logs
- Consult with operations personnel to ensure the secure configuration and maintenance of Bluedrop's production environment
- Respond to alerts related to security events on Bluedrop systems
- Manage security incidents
- Acquire and analyze threat intelligence
- Coordinate penetration testing
- Manage vulnerability scanning and remediation

4 Policies and Standards

Bluedrop maintains a set of policies, standards, procedures, and work instructions ("security documents") that provide the Bluedrop employees with the established practices for operating. Our security documents help ensure that Bluedrop customers can rely on our employees to behave ethically and for our service to operate securely. These policies are living documents, they are regularly reviewed and updated as needed, and made available to all employees to whom they apply.

5 Audits, Compliance, and 3rd Party Assessments

Our security program is designed to address the vast majority of the requirements of common security standards. The solutions we provide are battle-tested and have met the highest levels of audit scrutiny related to data security, privacy/consent legislation, and web content accessibility guidelines. Please contact us for more information or to request copies of publicly available reports and certifications.

SOC 2 Type 2 Certification

Developed by the AICPA, SOC 2 is widely recognized as the gold standard in data security for SaaS companies. It demonstrates Bluedrop ISM's commitment to data security through the practices and procedures it follows for protecting against unauthorized access, maintaining the availability of its services, and protecting the confidential information of its customers.

PCI-DSS Adherence

Bluedrop ISM adheres to the PCI-DSS technical and operational standards to secure and protect credit card data. The Company uses industry-leading third-party payment card processors who have been audited by an independent PCI Qualified Security Assessor (QSA) and are certified as a PCI Level 1 Service Provider.

Penetration Testing and Vulnerability Assessments

Bluedrop engages independent entities to conduct regular application-level and infrastructure-level penetration tests and vulnerability assessments. Results of these tests are shared with Bluedrop management. Bluedrop's Information Security Committee reviews and prioritizes the reported findings and tracks them to resolution.

Threat & Risk Assessments

Threat and Risk Assessments (TRAs) are a critical tool used by organizations to understand the various threats to IT systems, determining the level of risk these systems are exposed to, and recommending the appropriate level of protection. Bluedrop has been subject to, and successfully passed, multiple TRAs administered by governments and regulators around the globe.

Privacy Impact Assessments

Bluedrop ISM has completed a host of Privacy Impact Assessments (PIAs). These assessments provide confidence to customers that our solutions meet legislative requirements related to privacy, and reduce the risk of improper or unauthorized collection, use, disclosure, retention or disposal of personal information.

Multi-Point Security

Bluedrop assesses the security risk of each software development project according to our Secure Development Lifecycle. Before completion of the design phase, Bluedrop undertakes an assessment to qualify the security risk of the software changes introduced. All code is checked into a version-controlled repository. Code changes are subject to peer review and continuous integration testing.

For the SkillsPass ISM Platform, Bluedrop's security team operates continuous application review and analysis using advanced tools and best practice security techniques.

Protecting Customer Data

The focus of Bluedrop's security program is to prevent unauthorized access to customer data. To this end, our team of dedicated security practitioners, working in partnership with peers across all of our teams, takes exhaustive steps to identify and mitigate risks, implement best practices, and constantly evaluate ways to improve.

Data Encryption in Transit and at Rest

Bluedrop transmits data over public networks using strong encryption. This includes data transmitted between Bluedrop clients and the Bluedrop service.

Bluedrop supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS protocols, encryption, and hashing algorithms, as supported by the clients. This applies to all types of data at rest within Bluedrop's systems.

Network Security

Customer data submitted into the Bluedrop services is only permitted to exist in Bluedrop's production network, its most tightly controlled network. Administrative access to systems within the production network is limited to those engineers with a special business need. Only those network protocols essential for delivery of Bluedrop's service to its users are open at Bluedrop's perimeter.

Changes to Bluedrop's production network configuration are restricted to authorized personnel. In Bluedrop's hosted production environment, control of network devices is retained by the hosting provider. For that reason, Bluedrop logs, monitors, and audits system calls and has developed alerts for system calls that indicate a potential intrusion.

Authorizing Access

To minimize the risk of data exposure, Bluedrop adheres to the principle of least privilege —employees are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. To ensure that users are so restricted, Bluedrop employs the following measures: All systems used at Bluedrop require users to authenticate, and users are granted unique identifiers for that purpose. Each user's access is reviewed at least quarterly to ensure the access granted is still appropriate for the user's current job responsibilities. Employees may be granted access to a small number of internal systems, by default upon hire. Requests for additional access follow a documented process and are approved by the responsible owner or manager.

Authentication

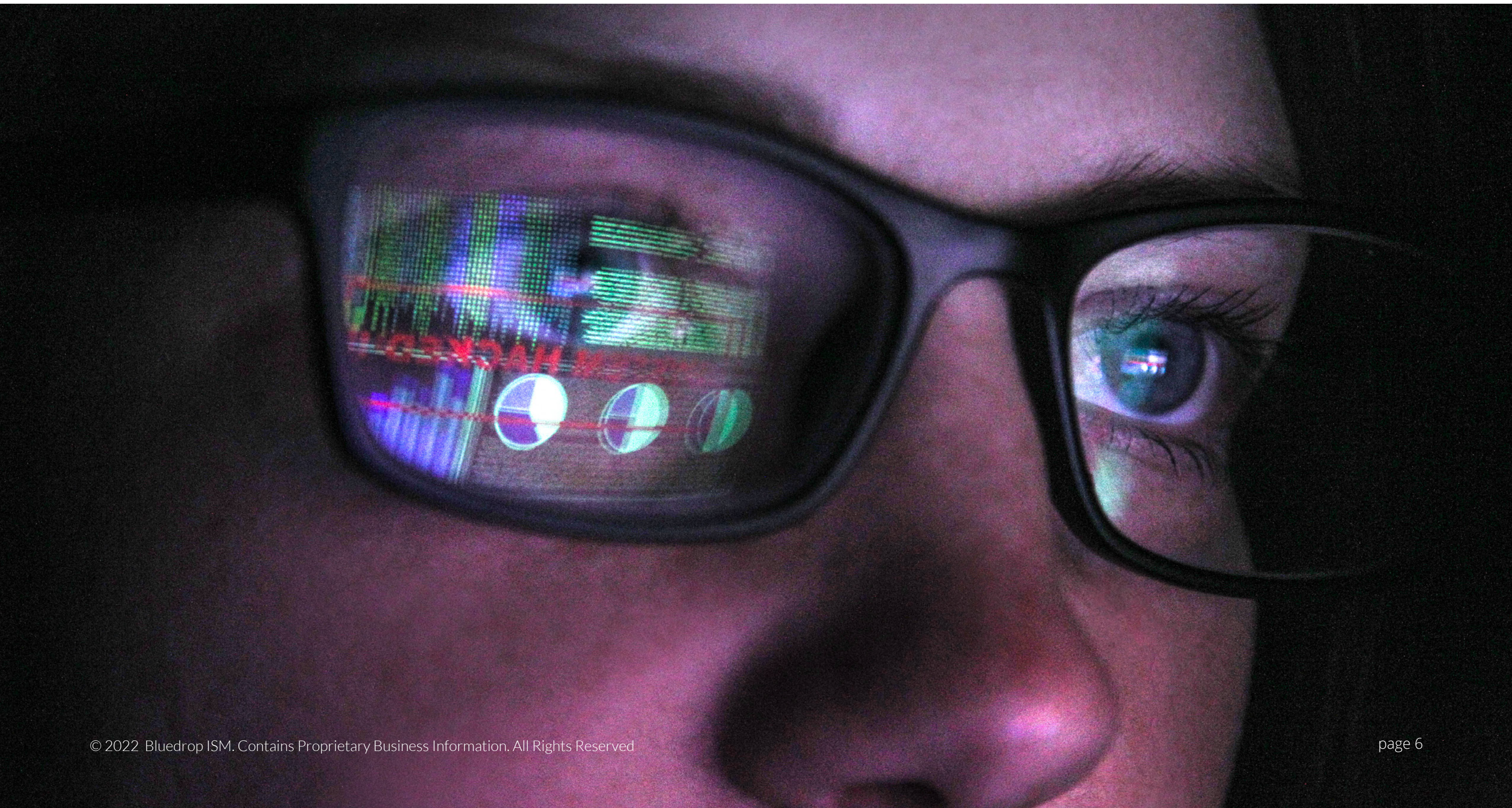
To further reduce the risk of unauthorized access to data, Bluedrop employs multi-factor authentication for administrative access to systems with more highly classified data. Where possible and appropriate, Bluedrop uses public and private key combinations for authentication. For example, at this time, administrative access to production servers requires operators to connect using an SSH key. Where passwords are used, multi-factor authentication is enabled for access to higher data classifications.

System Monitoring, Logging and Alerting

Bluedrop monitors servers, workstations, and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in Bluedrop's production network are logged. Bluedrop collects and stores internal (non-customer) production logs for analysis. Logs are protected and retained for at least one year. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. Alerts are examined and resolved based on documented priorities.

Responding to Security Incidents

Bluedrop has established policies and procedures for responding to potential security incidents. All incidents are managed by Bluedrop's dedicated Information Security Committee. Bluedrop defines the types of events that must be managed via the incident response process. Incidents are classified by severity. Incident response procedures are reviewed and updated at least annually.



Data and Media Disposal

Customer data is removed immediately upon deletion. Bluedrop hard deletes all information from currently running production systems. Bluedrop's infrastructure hosting provider is responsible for ensuring the removal of data from disks allocated to Bluedrop's use before they are repurposed.

Protecting Secrets

Bluedrop has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

Workstation Security

All workstations issued to employees are configured by Bluedrop to comply with our standards for security. These standards require all workstations to be properly configured, kept updated, and run monitoring software. Bluedrop's default configuration sets up workstations to encrypt data, have strong passwords and anti malware software installed to prevent infection.

Controlling System Operations and Continuous Deployment

We take a variety of steps to combat the introduction of malicious or erroneous code to our operating environment and protect against unauthorized access.

Controlling Change

To minimize the risk of data exposure, Bluedrop controls changes, especially changes to production systems, very carefully. Bluedrop applies change control requirements to systems that store data at higher levels of sensitivity. These requirements are designed to ensure that changes potentially impacting Customer Data are documented, tested, and approved before deployment.

Server Hardening

New servers deployed to production are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying Bluedrop's custom configuration settings to each server before use.

Disaster Recovery

Non-log production data are replicated among discrete operating environments to protect the availability of Bluedrop's service in the case of catastrophic events. Bluedrop performs restoration testing annually to ensure the completeness and accuracy of backup data.

Conclusion

We take security seriously at Bluedrop because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers and we work hard to maintain that trust.

> **There's no silver bullet solution with data security, a layered defence is the only viable defence."**
>
> *James Scott*

Bluedrop ISM

VISIT www.bluedrop.com
EMAIL isc@bluedrop.com