RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

**Technology Services**

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

# Vendor Statement of Compliance
# Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and

Jostens, Inc. ("Service Provider") on ________________ ("Effective Date").

**WHEREAS**, the LEA and the Service Provider entered into an agreement for Educational Technology services;

**WHEREAS**, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

**WHEREAS**, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

**NOW, THEREFORE,** the Parties agree as follows:

**Section I: General - All Data**

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ● No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ● No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ● No ○

**Section I: General - All Data** *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ● No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ● No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ● No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ● No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ● No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ● No ○

**Section II: AB1584 Compliance - Student Information Only**

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ◉ No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ◉ No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ◉ No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ◉ No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ◉ No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ◉ No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ◉ No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ◉ No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ◉ No ○

**Section III: SB 1177 SOPIPA Compliance - Student Information Only**

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ● No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ● No ○

3. Vendors cannot sell student information.

   Agree: Yes ● No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ● No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ● No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ● No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ● No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Tammy Whitaker
Print Name

Tammy Whitaker
Signature/Date

Laura Assem, 2/16/2022
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

## EXHIBITS

### Section 1.6: External Security

See attached Jostens Cybersecurity Compliance Program.

### Section 1.7: Internal Security

See attached Jostens Cybersecurity Compliance Program.

### Section II.2: Exporting of Student-Created Content

See attached Jostens Cybersecurity Compliance Program.

### Section II.4: Review and Correcting Personally Identifiable Information (PII)

Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify Jostens. Jostens agrees to facilitate such corrections within 21 days of receiving the District's written request.

# EXHIBITS

**Section II.5: Securing Student Data**

See attached Jostens Cybersecurity Compliance Program.

**Section II.6: Disclosure Notification**

See attached Jostens Cybersecurity Compliance Program.

**Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance**

See attached Jostens Cybersecurity Compliance Program.

**Section III.5: How Student Data is Protected:**

Data will be encrypted while in motion and at rest.

Reset Form

# CYBERSECURITY COMPLIANCE PROGRAM

## Jostens, Inc.

# Table of Contents

## Jostens Compliance Program Overview

### Jostens Compliance Policy

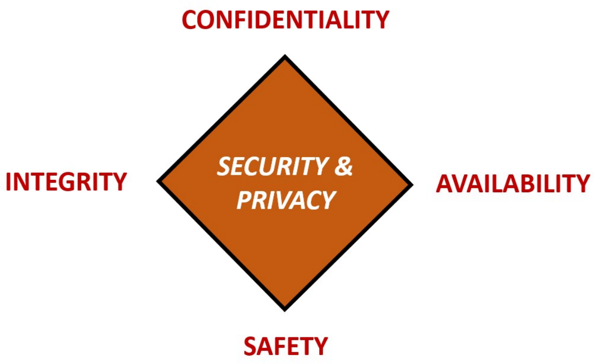
Jostens will protect the confidentiality, integrity, and availability of data and systems, regardless of how the data is created, distributed or stored. Jostens' security controls are tailored accordingly so that controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

### Management Direction for Cybersecurity

The objective of the Jostens Compliance Program is to provide cybersecurity requirements that are in accordance with Jostens' business requirements, as well as relevant laws and other legal obligations for data security and privacy. [1]

Jostens is committed to protecting its customers, employees, partners, and Jostens from damaging acts that are intentional or unintentional. Protecting Jostens data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensures the confidentiality, availability and integrity of the data:

Commensurate with risk, cybersecurity and privacy measures are implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction. The security of systems includes controls and safeguards to offset possible threats, as well as controls to ensures confidentiality, integrity, availability and safety:



- **Confidentiality** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **Integrity** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** – Availability addresses ensuring timely and reliable access to and use of information.
- **Safety** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Security measures are taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes against accidental loss or destruction.

### Scope

The requirements of the compliance program apply to all vendors, contractors, consultants, interns or other third-parties that support Jostens operations. This includes all stakeholders involved in transmitting, processing and storing Jostens data.

### Cybersecurity Practices Alignment

The National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF) represents leading industry-accepted best practices for cybersecurity.[2] Therefore, Jostens' minimum security requirements are consistent with NIST CSF controls to ensure due care and due diligence in maintaining its cybersecurity program.

[1] ISO/IEC 27002:2013 – 5.1

[2] NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

# CYBERSECURITY RESPONSIBILITIES

## HUMAN RESOURCES SECURITY

1. Requirements for Employment: Jostens maintains contractual agreements with employees, contractors, consultants and/or other third-party staff that formally documents their responsibilities for cybersecurity.

2. Roles and Responsibilities: Jostens defines and documents security roles and responsibilities of employees, contractors and third-party users to incorporate Jostens' data protection control requirements, to the extent permitted by applicable law:
   a. All employees, contractors, and third-party users are notified of the consequences for not following your security policy in handling Jostens data.
   b. All assets used to manage or store Jostens data are protected against unauthorized access, disclosure, modification, destruction or interference.
   c. All employees, contractors and third-party users are provided with education and training in privacy and security procedures and the correct information processing requirements.
   d. All personnel with access to sensitive Personally Identifiable Information (sPII) must complete a privacy training class and be knowledgeable of any specific privacy requirements for the data being handled. Refresher training is required at least on an annual basis.

3. Assigned Ownership: Jostens assigns ownership of critical and sensitive information, business applications, computer systems and networks to individuals (e.g., business managers) and document the responsibilities of these assigned owners.
   a. Responsibilities for protecting critical and sensitive information, business applications, computer systems and networks are communicated to and accepted by owners.

4. Personnel Screening: Jostens ensures a secure workforce. Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations, and ethics and are proportional to the business requirements and the classification of the information that may be accessed.

5. Staff Agreements: Jostens establishes agreements with employees that specify cybersecurity responsibilities. This agreement is incorporated into the contracts of employees, contractors, consultants and/or other third-party staff and taken into account when screening applicants for employment.

## CYBERSECURITY EDUCATION & AWARENESS

1. Cybersecurity Awareness: Jostens employees, contractors, consultants and/or other third-party staff are made aware of the key elements of cybersecurity, why it is needed, and understand their personal cybersecurity responsibilities. A security awareness program is undertaken to promote security awareness to all individuals who have access to the information and systems of the enterprise.

2. Cybersecurity Education: Jostens employees, contractors, consultants and/or other third-party staff are trained in how to run systems correctly, as well as how to develop and apply security controls.

## INFORMATION RISK ANALYSIS

1. Risk Analysis: Jostens performs information risk assessments of critical areas of its business to identify key information risks and determine the controls required to keep those risks within acceptable limits.
   a. Assessments must include, but are not limited to:
      i. Business environments;
      ii. Business processes;
      iii. Business applications (including those under development);
      iv. Computer systems, and
      v. Networks.

## Asset Management

1. Classification: Jostens utilizes a cybersecurity classification scheme that applies throughout the enterprise.

2. Asset Management: Jostens manages essential information about hardware, software, and data flows/extracts/interfaces (e.g., unique identifiers, version numbers, data recipients, physical locations) in inventory:
    a. An appropriate set of procedures for labeling and handling has been developed and implemented.
    b. Personal use of Jostens equipment and data is not allowed.

3. Handling Information: Jostens ensures additional protection is provided for handling sensitive material or transferring sensitive information.
    a. Files containing personal information or business sensitive information are transferred (e.g., email, faxes, etc.) via secure/encrypted file transfer protocols;
    b. Sensitive information is encrypted on all devices, including portable devices, such as laptops, portable media (flash drives) and data backups; and
    c. Jostens' minimum encryption requirement is 128-bit AES.

4. Supply Chain: Jostens ensures that reliable and approved hardware and software are acquired that follows consideration of security requirements. Vigilance are maintained to prevent counterfeit hardware and software from being used anywhere in the enterprise.

## Identity and Access Management

1. Access Control: Jostens restricts access to the application and associated information to authorized individuals. This are enforced accordingly to ensures that only authorized individuals to gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

2. User Authorization: Jostens ensures that all users have authorization before they are granted access privileges.
    a. User access privileges are reviewed at least every six (6) months; and
    b. Access are revoked immediately upon change in role or employment status.

3. User Authentication: Jostens ensures strong user authentication is implemented throughout the enterprise:
    a. All users are authenticated by an individual identifier, not group or shared identifiers; and
    b. Strong authentication mechanisms are used in conjunction with the identifier (e.g., strong passwords, smart cards or biometric devices) before the user can gain access to systems or data.

4. Privileged Accounts: Jostens ensures that accounts with privileged access are separate from a user's normal, non-privileged account.

5. Off-Premise Access Control: Whenever technically feasible, Jostens ensures cloud solutions offer the option to be federated to Jostens systems for authentication using Jostens credentials.

## Physical and Environmental Security

1. Facilities: Jostens secures facilities where Jostens data is stored, processed or transmitted:
    a. The number of entrances to the information processing facilities in which Jostens data is stored are limited.
        i. Every entrance into these areas requires screening. (e.g., security guard, badge reader, electronic lock, a monitored closed caption television (CCTV)).
        ii. Access logs are recorded and maintained.
    b. Physical access is restricted to those with a business need.
        i. Access lists are reviewed and updated at least once per quarter.
    c. Process, training, and policies are in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.
    d. Emergency exits in controlled areas must sound an alarm when opened and include automatic closure.
        i. Any alarms must trigger an emergency response.

2. Physical Protection: Jostens actively manages the physical security controls and ensures all buildings throughout the enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) are physically protected from unauthorized access.

3. Hazard Protection: Jostens ensures computer equipment and facilities are protected against natural and man-made hazards.

4. Power Supplies: Jostens protects critical computer equipment and facilities against power outages.

## System Configuration

1. Host System Configuration: Jostens configures host systems according to an industry standard.
   a. Systems are configured to function as required and to prevent unauthorized actions.
   b. Examples of best practice configuration include, but are not limited to:
      i. Center for Internet Security (CIS)
      ii. US Department of Defense Secure Technical Implementation Guides (STIGs)
      iii. OEM best practices (e.g., Microsoft, VMware, Oracle, etc.)

2. Mobile Devices: Jostens maintains policies, standards, and procedures covering the use of mobile/portable devices.
   a. The use of mobile devices (e.g., smartphone, iPad, tablet, USB memory sticks, external hard disk drives, MP3 players, e-book readers, etc.) are:
      i. Subject to approval; and
      ii. Access is restricted.
   b. Controls are implemented to ensures that sensitive information stored on these devices is protected from unauthorized disclosure.

## System Monitoring

1. Event Logging: Jostens logs all key cybersecurity events, including but not limited to:
   a. All actions taken by any individual with root or administrative privileges;
   b. Access to all audit trails;
   c. Invalid logical access attempts;
   d. All individual user accesses to cardholder data;
   e. Use of and changes to identification and authentication mechanisms, including but not limited to:
   f. Creation of new privileged accounts and elevation of privileges; and
   g. All changes, additions, or deletions to accounts with root or administrative privileges;
   h. Initialization, stopping, or pausing of the audit logs; and
   i. Creation and deletion of system-level objects.

2. System Network Monitoring: Jostens implements a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes:
   a. Reviewing the following, at least daily:
   b. All security events;
   c. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
   d. Logs of all critical system components; and
   e. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
      i. Firewalls;
      ii. Intrusion Detection Systems (IDS);
      iii. Intrusion Prevention Systems (IPS); and
      iv. Authentication servers (e.g., Active Directory domain controllers); and
   f. Following up exceptions and anomalies identified during the review process.

3. Intrusion Detection / Prevention: Jostens implements and monitors Intrusion Detection System (IDS) mechanisms on all critical systems and networks.

## Network Security

1. Defense In Depth (DiD): Jostens secures its computer networks using multiple layers of access controls to protect against unauthorized access. In particular:
    a. Group network servers, applications, data, and users into security domains;
    b. Establish appropriate access requirements within and between each security domain; and
    c. Implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.

2. Network Controls: Jostens ensures that all data and communications networks are secured to ensures the transmission of data is kept confidential.
    a. Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed;
    b. Network segments connected to the Internet are protected by a firewall which is configured to secure all devices behind it;
    c. Network segments where Jostens data resides are isolated from non-Jostens data, logically or physically unless approved by Jostens Security;
    d. User connection capability are documented with regard to messaging, electronic mail, file transfer, interactive access, and application access;
    e. All production servers are located in a secure, access-controlled location;
    f. Firewalls are configured properly to address all reasonably-known security concerns;
    g. Infrastructure diagrams, documentation, and configurations are up to date, controlled and available to assist in issue resolution; and
    h. Systems must have the ability to detect a potential hostile attack. (e.g., IDS/IPS)
        i. All systems are updated to the current release and actively monitored.

3. Wireless Access: Wireless access are authorized, authenticated, encrypted and permitted only from approved locations.

4. Remote Access: Remote access to a network containing Jostens data are done via a secure connection (e.g., VPN).
    a. All extranet connectivity into Jostens are through Jostens-approved and authorized secure remote connections.

## Cryptography

1. Cryptography: Jostens cryptographic solutions must:
    a. Meet or exceed Jostens' minimum encryption requirement of 128-bit AES; and
    b. Protect the confidentiality of sensitive information that is subject to legal and regulatory-related encryption requirements.

2. Cryptographic Key Management: Jostens manages cryptographic keys, in accordance with industry-recognized leading practices for key management:
    a. Documented standards and procedures must exist; and
    b. Cryptographic keys are protected against unauthorized access or destruction to ensures that these keys are not compromised (e.g., through loss, corruption or disclosure).

## Information Privacy

1. Information Privacy: Jostens establishes responsibilities for managing information privacy and data security controls for handling sensitive Personally Identifiable Information (sPII).

2. Alignment with Jostens Privacy: Jostens ensures sPII is collected, used, stored, transferred, and destroyed according to Jostens' privacy requirements.

## Malware Protection

1. Malware Controls: Jostens implements and manages enterprise-wide detection, prevention and recovery controls to protect against malware that includes having procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.

2. Malware Prevention: Jostens ensures the installation and regular update of malware detection and repair software to scan systems and media as a precautionary control, or on a routine basis. The scan carried out should include:
    a. Scan any files received over networks or via any form of storage medium, for malware before use;
    b. Scan electronic mail attachments and downloads for malware before use; and
    c. Scan web pages for malware.

## Vulnerability Management

1. Vulnerability Management: Jostens ensures a vulnerability management program exists to eliminate vulnerabilities that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). This includes, but is not limited to:
    a. Vulnerability remediation;
    b. Software and firmware patching; and
    c. Hardware maintenance.

2. Web-Enabled Applications: Jostens implements and manages specialized technical controls for web-enabled applications to ensures that the increased risks associated with web-enabled applications are minimized:
    a. All internets facing websites are scanned for security vulnerabilities that potentially open the site up to malicious behavior.
    b. Jostens' minimum list of validation is the Open Web Application Security Project (OWASP) Top 10 vulnerabilities (e.g., cross-site scripting (XSS), SQL injection, Admin access, open directories, insecure data transfer, etc.).

## Communications & Operations Management

1. Communications Security: Jostens supports standards and procedures that ensures confidentiality, integrity, and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

2. Operations Management: Jostens maintains overall operational control and visibility into all security aspects of how data is processed, stored and transmitted:
    a. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility;
    b. Jostens have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process; and
    c. Vendors are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

## System Acquisition, Development & Maintenance

1. Specification of Requirements: Jostens takes into consideration the cybersecurity requirements for the system under development when designing the system to ensures Jostens' business requirements (including those for cybersecurity) are documented and agreed upon before detailed design commences.

2. Quality Assurance: Jostens ensures quality assurance activities are performed for critical security controls during the development lifecycle.

3. Testing: Jostens ensures that all elements of a system (e.g., application software packages, system software, hardware, and services) are rigorously tested before the system is promoted to a production environment.

4. Test Data: Jostens ensures any sensitive Jostens business information copied from the production environment are protected by:
   a. Depersonalizing sensitive business information;
   b. Restricting access to business information in the development environment; and
   c. Erasing copies of Jostens business information once testing is complete.

5. Development Methodologies and Environment: Jostens development activities are:
   a. Carried out in accordance with a documented system development methodology;
   b. Performed in specialized development environments;
   c. Isolated from production environments; and
   d. Protected against disruption and disclosure of information.

6. System Design / Build: Jostens ensures system build activities are:
   a. Carried out in accordance with industry-recognized leading practices (e.g., OWASP);
   b. Performed by individuals provided with adequate skills/tools; and
   c. Inspected to identify unauthorized modifications or changes which may compromise security controls.

7. Installation Process: Jostens ensures that newly-promoted systems to the production environment are installed in accordance with the Jostens documented installation process.

8. Post-implementation Review: Jostens ensures a post-implementation review is conducted for all newly-promoted systems to the production environment.

9. Secure Destruction: Jostens ensures methods of destruction are formally implemented, based on the type of media:
   a. Physical, paper-based media;
   b. Physical, digital media; and
   c. Electronic, digital data.

10. Lifecycle Management: Jostens defines the End of Life (EOL) process for all systems and applications which could include date of EOL and any business triggers that may result in updated EOL date;

## Change Management

1. Change Control: Jostens documents and manages operating procedures for its change control process(es).

2. Change Management: Jostens ensures that changes to any systems, applications or networks, including “emergency” changes, are reviewed, tested, approved and applied using a change management process.

3. Change Documentation Retention: Jostens ensures that documentation of changes is retained for at least three hundred and sixty-five (365) days.

## Cybersecurity Incident Management

1. Incident Management: Jostens documents all cybersecurity incidents and maintain a documented cybersecurity event management process that covers the incident response, escalation, and remediation of Cybersecurity events and incidents.

2. Forensic Investigations: Jostens has an established process for managing incidents that require forensic investigation.

## Disaster Recovery

1. Disaster Recovery: Jostens develops, supports and routinely tests Disaster Recovery (DR) activities that address all reasonably-foreseen contingency arrangements.

2. Resilience: Jostens applications, systems, and networks are run on robust, reliable hardware and software, supported by alternative hardware or duplicate facilities.

3. Data Backups: Jostens ensures that backups of essential information and software are performed on a regular basis, according to a defined cycle discussed with and approved by Jostens.

## Processing Facilities

1. Comingling of Data: Jostens ensures that when Jostens business information is co-located with non-Jostens data, (e.g., virtual servers, cloud solutions, etc.) the non-Jostens data must at least be logically separated from Jostens business information.

2. Virtualization & Cloud Solutions: Jostens may utilize a cloud solution, which must adhere to the same security principles required by Jostens IT security policies and applicable government regulations, laws, or directives as used throughout the enterprise:
   a. The geographic location of provider infrastructure resources is known to Jostens. Jostens is in control of the data location to ensure compliance with local laws that restrict the cross-border flow of data.
   b. Vendors providing cloud services must:
      i. Provide a process for data destruction and secure deletion of any and all Jostens data as needed;
      ii. Have an established method of encrypting sensitive data in storage and in transit following industry-recognized leading practices;
      iii. Securely handle Jostens related data, compute resources, virtual machines resources by providing logical isolation and secure migration;
      iv. Include methods or options for multi-factor authentication for cloud administrator roles;
      v. Provide Jostens the capability to fully audit Jostens user access and activity within the cloud service. Audit logs are capable of being exported from the cloud service;
      vi. Limit employee access to the least privilege needed to perform their duties.
      vii. Maintain documented audits or established compliance roadmaps in alignment with Industry Standard Certifications for Cloud Security. Examples include ISO27001/2, SSAE16, FEDRAMP, CSA STAR, FIPS 140-2, and Open Data Alliance;
      viii. Demonstrate adherence to Security Development best practices for all code, APIs, and applications deployed and implemented in support of the cloud service;
      ix. Process and advise Jostens of any security breach involving Jostens data or services utilized by Jostens; and
      x. Provide Jostens with the means to monitor in near real-time service and resource availability; and
   c. All access to cloud computing sites must encrypt data in transit.
      i. Any Jostens data stored in a cloud environment is encrypted so that data cannot be read by other users in a multi-tenant environment.

## Vendor Management

1. Outsourcing: Jostens operates a formal process to address due care and due diligence considerations in the selection and management of third-party vendors:
   a. These third-party vendors must sign agreements that specify the security requirements to be met before commencing work on behalf of Jostens that could have an impact on Jostens' business operations with the vendor;
   b. These security requirements must align with the provisions expected of Jostens from vendor; and
   c. All subcontracted activities involving Jostens information are approved and secured by vendor.

2. VENDOR Exit Strategy: Jostens ensures a documented termination of service process is in place that ensures Jostens business data is recoverable if Jostens terminates a service agreement with a third-party vendor.

3. Indemnification: Jostens addresses indemnification considerations with third-party vendors that could have an impact on Jostens' business operations with the vendor.

## COMPLIANCE

1. Statutory / Regulatory / Contractual Compliance. Jostens maintains a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements. Examples include but are not limited to FERPA, COPPA, CCPA, PCI DSS, HIPAA, and SOX.

2. Compliance Status: Jostens has a process to document non-compliance of any statutory, regulatory or contractual requirement:
    a. Jostens identify and quantify the risks and mitigation plans and documents the business decision for alternate controls or risk acceptance; and
    b. The mitigation plan and business decision are signed off by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability.

3. Breach Notification: Jostens maintains a documented breach notification process that meets all applicable legal and contractual requirements.

4. Payment Card Industry Data Security Standard (PCI DSS): Jostens does not store customers' cardholder data; however, Jostens falls within scope of PCI DSS compliance and therefore:
    a. Maintains documented compliance with the most current version of the PCI DSS;
    b. Conducts quarterly network scans by an Approved Scanning Vendor (ASV); and
    c. Obtains a Report of Compliance (ROC) from an annual on-site PCI Data Security Assessment with a Qualified Security Assessor (QSA).

## GLOSSARY: ACRONYMS & DEFINITIONS

### ACRONYMS

AD. Active Directory

APT. Advanced Persistent Threat

BCP. Business Continuity Plan

CDE. Cardholder Data Environment

CERT. Computer Emergency Response Team

CIRT. Computer Incident Response Team

COOP. Continuity of Operations Plan

CTI. Controlled Technical Information [3]

CUI. Controlled Unclassified Information [4]

DAC. Discretionary Access Control

DISA. Defense Cybersecurity Agency

DLP. Data Loss Prevention

DRP. Disaster Recovery Plan

EAP. Extensible Authentication Protocol

EPHI. Electronic Protected Health Information

FICAM. Federal Identity, Credential, and Access Management

FIM. File Integrity Monitor

GDPR. General Data Protection Regulation

HIPAA. Health Insurance Portability and Accountability Act

IRP. Incident Response Plan

ISMS. Cybersecurity Management System

ISO. International Organization for Standardization

LDAP. Lightweight Directory Authentication Protocol

MAC. Media Access Control

NIST. National Institute of Standards and Technology

PCI DSS. Payment Card Industry Data Security Standard

PDCA. Plan-Do-Check-Act

PIV. Personal Identity Verification

RBAC. Role-Based Access Control

TLS. Transport Layer Security

### DEFINITIONS

Jostens recognizes two sources for authoritative definitions:

- Unified Compliance Framework (UCF) Compliance Library[5]
- The National Institute of Standards and Technology (NIST) IR 7298, Revision 2, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms. [6]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (i.e., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method, or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[7]

[3] CUI Registry - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html

[4] CUI Registry - https://www.archives.gov/cui/registry/category-list

[5] UCF Compliance Library - https://compliancedictionary.com

[6] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[7] ISO/IEC/IEEE 29148