REDSHELF, INC.
CAMPUS SERVICES AGREEMENT

This Campus Services Agreement (the "Agreement") is executed as of the last date set forth below ("Effective Date"), by and between RedShelf, Inc., a Delaware corporation, with offices at 500 N. Dearborn St., Suite 1200, Chicago, IL 60654. ("RedShelf") and Black Hawk College , whose address is 6600 34th Avenue, Moline, Illinois 61265 ("Customer").

1. RedShelf Services.

1.1 Access to Academic Course Content. RedShelf will make third party Academic Course Content and Custom Content available for purchase and rent to Customer's end users through the Branded Interface (defined below). "Academic Course Content" means textbooks, custom textbooks, publisher access codes, course packets, course readers, lab manuals, note packets, and other content. RedShelf will use commercially reasonable measures to ensure that the Academic Course Content is available to Customer's end users through the Branded Interface, although RedShelf will not be liable for damages caused by interruptions of service.

1.2 Distribution of Custom Content. At Customer's request, RedShelf will distribute Custom Content through the Branded Interface. "Custom Content" means Academic Course Content that is developed by Customer and distributed on the Branded Interface, such as course packets, course readers, lab manuals, note packets, and other content. Posting of Custom Content generated by Customer is the responsibility of Customer. On a per title basis, Custom Content posted to the Branded Interface will be stored by RedShelf for the lesser of either the term determined by Customer at posting or one (1) year from last access of the title by a student/user. Customer may request existing Custom Content to be removed for sale or substituted with reasonable notice and for any reason.

1.3 Branded Interface. RedShelf will create and maintain a branded digital Academic Course Content delivery interface (the "Branded Interface") where end users purchase and access Academic Course Content. RedShelf ensures the Branded Interface is and will continue to be compliant with Payment Card Industry Data Security Standard (PCI DSS). When requested, RedShelf will provide Customer with Attestation of Compliance (AOC). Customer will be responsible for embedding the Branded Interface, which will be available through one or more URL links, into the Customer's website.

1.4 Customer Service on Branded Interface. RedShelf agrees to be responsible for customer service needs related to the use of the Branded Interface or any of the technology contained within the Branded Interface. RedShelf customer service contact information will be provided on the Branded Interface.

1.5 Inclusive Access. The "Inclusive Access" business model is an option that includes the cost of Academic Course Content as a course fee billed on student accounts or includes the cost of Academic Course Content within tuition. If requested by the Customer for a course, RedShelf will work with publishers to seek preferred pricing for Academic Course Content and will inform Customer of available pricing, in writing (including email), prior to the completion of the order. RedShelf will also communicate the net amount due to the publisher on each title of Academic Course Content (the "Net Publisher Payment") and any Inclusive Access Fees due to RedShelf. Customer will then make payment to RedShelf as stated in 2.3 and 2.8. RedShelf will then remit payment due to the publishers or owners of the Academic Course Content in use by Customer.

2. RedShelf Fees; Pricing; Payment Terms.

2.1 Academic Course Content Purchases – Customer Processes Payment. For purchases of Academic Course Content through the Branded Interface that are processed by Customer, Customer will collect the retail price listed by RedShelf or the related publisher for such Academic Course Content and remit to RedShelf 90% of such retail price. Customer agrees not to modify prices provided by RedShelf through the Branded Interface.

2.2 Academic Course Content Purchases – RedShelf Processes Payment. For purchases of Academic Course Content through the Branded Interface that are processed by RedShelf, RedShelf will collect the retail price listed on the Branded Interface and remit to Customer a fee equal to 10% of such retail price.

2.3 Inclusive Access. For Customers using the Branded Interface to distribute Academic Course Content through an Inclusive Access model, Customer will remit the Net Publisher Payment plus the Inclusive Access Fee. Unless otherwise agreed to in writing (including email), for digital textbooks, the "Inclusive Access Fee" will be a 10% margin placed on the Net Publisher Payment. For publisher access codes, the "Inclusive Access Fee" will be a 5% margin placed on the Net Publisher Payment. Inclusive Access Fees cover the cost of the tools and features RedShelf provides the Customer to support the Inclusive Access model. For all other Academic Course Content, RedShelf and Customer will mutually agree upon the Inclusive Access Fee in writing.

2.4 Custom Content Purchases – Customer Processes Payment. For purchases of Custom Content through the Branded Interface that are processed by Customer, Customer will collect the retail price set by Customer for such Custom Content and remit to RedShelf 10% of such retail price as "Custom Content Fee".

2.5 Custom Content Purchases – RedShelf Processes Payment. For purchases of Custom Content through the Branded Interface that are processed by RedShelf, RedShelf will collect the retail price set by Customer and remit to Customer 90% of such retail price, retaining 10% as "Custom Content Fee".

2.6 Academic Course Content Pricing Changes. RedShelf will update the prices for Academic Course Content when notified and as required by the publishers of Academic Course Content. RedShelf will provide the Customer with advance notice of any coming price changes as soon as reasonably practical.

2.7 Returns. Except for purchases made through the Inclusive Access Program pursuant to Section 2.3, Customer and RedShelf agree that end users may return Academic Course Content in accordance with RedShelf's then-current return policy. Each Party agrees that it must return any fees that are paid with respect to Academic Course Content that is returned in accordance with such return policy. The Statement of Activity will list returned Academic Course Content and adjust the fee due to Customer or RedShelf, as applicable.

2.8 Statement of Activity. Within twenty (20) days of the close of each calendar month, RedShelf will provide the Customer with a statement of activity for the immediately preceding month, including sales processed by RedShelf, sales processed by Customer, any returns, and fees earned by each Party (each, a "Statement of Activity"). RedShelf and Customer agree that any amounts due to the other Party will be paid within thirty (30) days of each Statement of Activity.

2.9 Taxes. The Party collecting payments on the Academic Course Content shall be responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state or local governmental entity on sales of such Academic Course Content.

2.10 Set-Off Permitted by RedShelf. Without prejudice to any other right or remedy RedShelf has or may have, RedShelf may, in good faith and without notice to Customer, set-off or recoup any liability RedShelf owes to Customer against any liability Customer owes to RedShelf, whether either liability is matured or unmatured.

2.11 Disputes. In the event that Customer believes there is an error on a Statement of Activity, it must notify RedShelf in writing of such believed error (along with substantiating documentation) within fifteen (15) days from the date of receipt of such Statement of Activity, after which RedShelf and Customer agree that RedShelf has no obligation to reconcile or honor any dispute over such Statement of Activity. Customer will be deemed to have accepted all Statements of Activity for which Customer does not provide timely notification of disputes in accordance with this Section 2.11. The Parties will seek to resolve all such disputes expeditiously and in good faith.

3. Intellectual Property.

3.1 License Grant to RedShelf. During the Term, Customer grants to RedShelf a limited, non-exclusive, non-sublicenseable license to use Customer's trademark in connection with the Branded Interface and RedShelf's performance of the services under this Agreement.

3.2 Intellectual Property of RedShelf. All intellectual property rights, including copyrights, patents, patent disclosures and inventions (whether patentable or not), trademarks, service marks, trade secrets, know-how and other confidential information, trade dress, trade names, logos, corporate names and domain names, together with all of the goodwill associated therewith, derivative works and all other rights (collectively, "Intellectual Property Rights") in and to all documents, work product and other materials that are delivered to Customer under this Agreement or prepared by or on behalf of RedShelf in the course of performing under this Agreement, including any items developed hereunder for the Branded Interface (such as the RedShelf digital platform, API and software) shall be owned by RedShelf.

3.3 Custom Content. To the extent that Customer distributes Custom Content through the Branded Interface, Customer agrees as follows:

(a) As between the Customer and RedShelf, Customer will own the Custom Content, and set prices and DRM restrictions.

(b) Customer hereby represents and warrants that it has all rights, titles, or interests in (including, but not limited to all necessary copyright and author permissions) the Custom Content. Customer further represents and warrants that it has the right to distribute the Custom Content on the Branded Interface, and has the authority and the legal right to permit RedShelf to perform the services described in this Agreement and contemplated hereby.

4. Usage Data.

4.1 General Analytic Data. RedShelf may provide Customer with general analytic data related to the Branded Interface, such as unique visitors, total visitors, and analytics on usage and timing.

4.2 Information Covered by FERPA (Inclusive Access only). With respect to Customer or its end users' use of the Branded Interface through the Inclusive Access model, RedShelf and the Customer agree to the following:

(a) In the course of providing services under an Inclusive Access model to Customer, RedShelf may have access to student education records that are subject to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, et seq. and the regulations promulgated thereunder. Both Parties are committed to fully comply with all FERPA-requirements, as outlined in Exhibit A to this Agreement.

(b) RedShelf is committed to its data security plan, attached to this agreement as Exhibit B. RedShelf preserves the right to update its data security plan from time to time, in order to stay up to date with current industry standards. Customer will be notified of any future updates of said security plan, by RedShelf sending a new Exhibit B to Customer by email.

5. Limitation of Liability; Indemnification.

5.1 REDSHELF MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, FROM A COURSE OF PERFORMANCE OR DEALING, TRADE USAGE, OR OF UNINTERRUPTED OPERATION WITHOUT ERROR, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THERE IS NO WARRANTY AGAINST INTERFERENCE WITH CUSTOMER'S ENJOYMENT OF ANY INFORMATION (INCLUDING DATA AND COMPUTER PROGRAMS) OR AGAINST INFRINGEMENT. REDSHELF MAKES NO GUARANTEES WITH REGARD TO THE RESULTS OBTAINED FROM THE OPERATION OR USE BY CUSTOMER OF THE BRANDED INTERFACE. REDSHELF SHALL HAVE NO LIABILITY WHATSOEVER FOR ANY COVER OR SET-OFF NOR FOR ANY INDIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR PUNITIVE DAMAGES, INCLUDING LOST PROFITS, EVEN IF REDSHELF HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5.2 IN NO EVENT SHALL REDSHELF'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING OUT OF OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EXCEED THE AGGREGATE AMOUNTS PAID OR PAYABLE TO REDSHELF PURSUANT TO THIS AGREEMENT IN THE SIX MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

5.3 Indemnification. Each party to this agreement will indemnify, hold harmless, and defendthe other party and its officers, directors, employees, agents, affiliates, successors and permitted assigns (collectively, " Indemnified Party") against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, and the costs and expenses of enforcing any right to indemnification under this Agreement and the cost of pursuing any insurance, (collectively, "Losses"), incurred by the Indemnified Party solely relating to, arising out of or resulting from third party claims, or from gross negligence or willful misconduct in connection with this Agreement.

6. Term; Termination and Survival.

6.1 Term. This Agreement shall commence as of the Effective Date and shall continue thereafter until terminated pursuant to this Section 6 (the "Term").

6.2 Termination for Cause. Either Party may terminate this Agreement, effective upon written notice to the other Party, if the defaulting Party (a) materially breaches this Agreement, and such breach is incapable of cure, or with respect to a material breach capable of cure, the defaulting Party does not cure such breach within fifteen (15) days after receipt of written notice of such breach from the other Party; (b) becomes insolvent or admits its inability to pay its debts generally as they become due; (c) becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency law, which is not fully stayed within seven (7) days or is not dismissed or vacated within forty-five (45) days after filing; (d) is dissolved or liquidated or takes any corporate action for such purpose; (e) makes a general assignment for the benefit of creditors; (f) has a receiver, trustee, custodian or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

6.3 Termination for Convenience. Either Party, in its sole discretion, may terminate this Agreement at any time without cause, by providing at least thirty (30) days' prior written notice to the other Party. Within fifteen (15) days of the termination date, Parties agree to make final payments on all amounts due under this Agreement.

6.4 Survival. The rights and obligations of the Parties set forth in this Section 6 and Sections 2, 3, 4, 5 and 7, and any right or obligation of the Parties in this Agreement which, by its nature, should survive termination or expiration of this Agreement, including a student's right to access their content through the duration of their purchase, will survive any such termination or expiration of this Agreement.

7. Miscellaneous

7.1 Non-Solicitation. During the period beginning with the Effective Date and ending twelve (12) months after termination, the parties will not, without the written consent of the other party, directly or indirectly, solicit, induce, recruit, encourage or otherwise endeavor to cause or attempt to cause any employee, contractor, or business partner of either party to terminate or modify their current employment relationship, nor interfere with those relationships.

7.2 Entire Agreement. This Agreement, including and together with exhibits, schedules, attachments and appendices, constitutes the sole and entire agreement of the Parties with respect to the subject matter contained in this Agreement, and supersedes all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, regarding such subject matter.

7.3 Notices. All notices, requests, demands, consents, instructions or other communications required or permitted hereunder shall be in writing and faxed, mailed or delivered to each Party at the respective addresses of the Parties set forth below, or at such other address or facsimile as the Parties may designate from time-to-time. Notices to RedShelf shall additionally be sent by e-mail to tim@redshelf.com. All such notices and communications will be deemed effectively given the earlier of (a) upon personal delivery to the Party to be notified, (b) when sent by confirmed electronic mail or facsimile if sent during normal business hours of the recipient, if not, then on the next business day, (c) five (5) days after having been sent by registered or certified mail, return receipt requested, postage prepaid, or (d) one (1) day after deposit with a nationally recognized overnight courier, specifying next day delivery, with written verification of receipt.

7.4 Severability. If any term or provision of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction.

7.5 Amendment. No amendment to this Agreement is effective unless it is in writing and signed by each party to this Agreement, provided, however, that RedShelf may modify or amend Sections 1 and 2 of this Agreement from time-to-time with thirty (30) days' prior written notice to Customer to reflect the then-current services and pricing offered by RedShelf.

7.6 Waiver. No waiver by any Party of any of the provisions of this Agreement shall be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power or privilege arising from this Agreement shall operate or be construed as a waiver thereof, nor shall any single or partial exercise of any right, remedy, power or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege.

7.7 Assignment. The parties shall not assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other party. Any purported assignment or delegation in violation of this Section 7.7 shall be null and void. No assignment or delegation shall relieve either party of any of its obligations under this Agreement. A party may assign any of its rights or delegate any of its obligations to any affiliate or to any person acquiring all or substantially all of that party's assets without the other party's consent.

7.8 Successors and Assigns. This Agreement is binding on and inures to the benefit of the Parties to this Agreement and their respective permitted successors and permitted assigns.

7.9 No Third-Party Beneficiaries. This Agreement benefits solely the Parties to this Agreement and their respective permitted successors and assigns and nothing in this Agreement, express or implied, confers on any other person any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

7.10 Choice of Law. This Agreement, including all exhibits, schedules, attachments and appendices attached to this Agreement, and all matters arising out of or relating to this Agreement, are governed by, and construed in accordance with, the laws of the State of Illinois, without regard to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the laws of any jurisdiction other than those of the State of Illinois.

7.11 Choice of Forum. Each Party hereby irrevocably and unconditionally consents to submit to the exclusive jurisdiction of the Courts of the State of Illinois and the United States of America located in the City of Chicago for any actions, suits or proceedings arising out of or relating to this Agreement and the transactions contemplated hereby (and each Party agrees not to commence any action, suit or proceeding relating thereto except in such courts), and further agree that any service of any process, summons, notice or document sent by U.S. registered mail to the address set forth in this Agreement shall be effective service of process for any action, suit or proceeding brought against a Party in any such court. Each Party hereby irrevocably and unconditionally waives any objection to the laying of venue of any action, suit or proceeding arising out of this Agreement or the transactions contemplated hereby, in the courts of the State of Illinois or the United States of America located in the City of Chicago, and hereby further irrevocably and unconditionally waive and agree not to plead or claim in such court that any such action, suit or proceeding brought in any such court has been brought in an inconvenient forum.

7.12 Counterparts. This Agreement may be executed in two (2) or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Counterparts may be delivered via facsimile, electronic mail (including pdf or any electronic signature complying with the U.S. federal ESIGN Act of 2000, e.g., www.docusign.com) or other transmission method and any counterpart so delivered shall be deemed to have been duly and validly delivered and be valid and effective for all purposes. Any Party delivering an electronic signature agrees that such electronic signature is the legally binding equivalent to such Party's handwritten signature and has the same validity and meaning as such Party's handwritten signature. Such Party further agrees that such Party will not, at any time in the future, repudiate the meaning of such electronic signature or claim that such electronic signature is not legally binding. Such Party further agrees that no certification authority or other third party verification is necessary to validate such electronic signature and that the lack of such certification or third party verification will not in any way affect the enforceability of such electronic signature or any resulting contract.

The Parties have executed this Agreement as of the date last written below.

For RedShelf;

Tim Haitaian

For Customer:

Mike G Meleg

SIGNATURES

Full name	Tim Haitaian	Full name	Mike Meleg
Company	RedShelf	Company	Black Hawk College
Title	CFO & Co-Founder	Title	Purchasing Manager
	Tim Haitaian		Mike G Meleg
	Signed on 3/07/2018		Signed on 3/05/2018

EXHIBIT A. FERPA-COMPLIANCE

All capitalized terms not otherwise defined herein have the meaning ascribed to same in the Agreement and the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, et seq. / 34 CFR Part 99 and the regulations promulgated thereunder.

1. **School Official – exception**

   a) To the extent that RedShelf has access to "Education Records" under this Agreement, it is deemed a "School Official," as each of these terms are defined under FERPA.

   b) Company confirms that pursuant to its current public "FERPA Rights Notice" as mentioned in 34 CFR § 99.7 CFR, RedShelf meets the criteria to be considered a 'School Official' with a 'Legitimate Educational Interest'.

   c) If Company would alter its FERPA Rights Notice as a result of which RedShelf possibly no longer meets the 'School Official' and 'Legitimate Educational Interest'-criteria, RedShelf shall not be held responsible nor accountable for any unlawfully accessed Personally Identifiable Information.

2. **Control over Data.** RedShelf will be under direct control of the Company with respect to use and maintenance of education records. Accordingly, parties agree that,

   a) in the event any person(s) seeks to access protected education records, whether in accordance with FERPA or other Federal or relevant state law or regulations, RedShelf will promptly inform Customer of such request in writing if allowed by law or judicial and/or administrative order. RedShelf shall not provide direct access to such data or information or respond to individual requests. RedShelf shall only retrieve such data or information upon receipt of, and in accordance with, written directions by Customer and shall only provide such data and information to Customer. It shall be Customer's sole responsibility to respond to requests for data or information received by RedShelf regarding Customer data or information. Should RedShelf receive a court order or lawfully issued subpoena seeking the release of such data or information, RedShelf shall provide prompt notification to Customer of its receipt of such court order or lawfully issued subpoena and shall immediately provide Customer with a copy of such court order or lawfully issued subpoena prior to releasing the requested data or information, if allowed by law or judicial and/or administrative order.

   b) If RedShelf experiences a security breach concerning any education record covered by this contract, then RedShelf will promptly notify Customer and take prompt steps to limit and mitigate such security breach to the extent possible. The Parties agree that any breach of the confidentiality obligation set forth in this Agreement may, at Customer's discretion, result in cancellation of further consideration for contract award and the eligibility for RedShelf to receive any information from Customer for a period of not less than five (5) years.

   c) Upon termination of this Agreement and written notice from Customer, RedShelf shall return and/or destroy all data or information received from Customer upon, and in accordance with, direction from Customer. RedShelf shall not retain copies of any data or information received from Customer once Customer has directed RedShelf as to how such information shall be returned to Customer and/or destroyed. Furthermore, RedShelf shall ensure that they dispose of any and all data or information received from Customer in a Customer-approved manner that maintains the confidentiality of the contents of such records (e.g. shredding paper records, erasing and reformatting hard drives, erasing and/or physically destroying any portable electronic devices).

3. **Authorized purpose only**

RedShelf will use the students' Personally Identifiable Information from their Education Records only for rendering the services it's been contracted for pursuant to the Agreement, namely providing students Customer's students with access to (a) all learning materials, tools and services that they purchased; and/or (b) all learning materials, tools and services pertaining to the course(s) they enrolled for through the Inclusive Access Program.

If RedShelf were to use any user data for any other purposes then the fulfillment of this Agreement, RedShelf will make sure such data is properly de-identified prior to such use. Such de-identified data will have all direct and indirect personal identifiers removed, including name, ID, date of birth, demographic information, location information, and school ID. RedShelf will not attempt to re-identify any de-identified data.

4. **Re-disclosure of PII.**

a) Except as required by law, RedShelf shall not disclose or share any education records or any Personally Identifiable Information contained therein, to any third party without the prior written consent of the student, unless permitted by the terms of this Agreement or any of its Exhibits.

b) Company authorizes RedShelf to share, on behalf of the Company:

(i) End Users' "Basic User Information" (students' name, email address and student ID), Usage Data (content and pages the student accessed on RedShelf, as well as the dates, times and durations such access) and User Content (any personally added content, including highlights, notes, flashcards, study guides, comments, shared content, feedback...) with relevant administrative and academic staff and faculty within the Company, which RedShelf may assume to be school officials as well, pursuant to CFR 34 § 99.31(a);

(ii) End Users' Basic User Information and Usage Data with Content holders and other educational service providers that are instrumental in the delivery of and reporting on the Content and services to Company's End Users, which RedShelf may assume to be school officials as well, pursuant to CFR 34 § 99.31(a).

c) If RedShelf were to share any data with any other third parties, RedShelf will make sure such data is properly de-identified prior to such disclosure, and to only share such de-identified data with third parties who agree not to attempt any re-identification.

EXHIBIT B - RedShelf Security Overview

RedShelf Security Overview

Oversight and Implementation of Information Security

RedShelf's Development Operations (DevOps) and Development Teams are responsible for security of information and systems. RedShelf extensively vets these team members through technical evaluations, background checks, and other methods to ensure employees who have access to any data are fully competent.

Employee Background Checks

RedShelf performs background checks, education checks, criminal history and reference checks.

RedShelf Data Hosting

RedShelf hosts its data on Amazon Web Services. All data is encrypted during transmission. Production database servers are never exposed to the internet and are only accessible through internal networks.

Data Center Redundancy

RedShelf has multiple availability zones in multiple regions for all components. Critical components are also replicated on another service (Google Container Engine) in case of any interruption with AWS.

Physical and Environmental Controls

No RedShelf employee has physical access to any server in RedShelf's environment.

Network Security Controls

All infrastructure components are inside of a VPC. Only HTTP traffic is allowed through a load-balancer. Only a single server allows SSH traffic which requires private key authentication and white-listed IP addresses. All user login attempts, and actions are logged in our central logging platform with alerts configured for unusual activity. All network traffic and AWS administrative operations are logged using Nginx, Loggly, and CloudTrail. Keys and passwords are periodically rotated for all engineering staff. When available, RedShelf requires two-factor authentication for login to any sensitive or critical component.

Patch Management

RedShelf is hosted on AWS so underlying infrastructure patches are applied automatically. RedShelf's AWS architecture configuration is managed using Salt formulas under source control. All changes must pass code review and testing before release.

Network Performance Monitoring

RedShelf uses a combination of New Relic, AWS CloudMetrics, and Loggly to monitor all network performance. Automated alerts are configured for high-latency, high error rates, and anomaly detection.

Encryption

RedShelf uses TLS and 2048-bit RSA encryption on all data transferred between services or internally.

SDLC Process

All code changes use the following process:

- A ticket is created for a requirement that must be implemented by the engineering team
- The ticket is reviewed by the team for planning, architecture analysis, and estimation
- A developer creates a change request for the proposed changes in a VCS
- The change request is reviewed by two staff members for performance, code style, and security
- A continuous integration server builds a Docker container using the change request and runs unit, integration, and acceptance tests. The Docker image is also pushed to DockerHub.
- DockerHub performs static security analysis of all packages and dependencies and reports any warnings or issues
- If the change request passes code review, continuous integration testing, and dependency analysis, it is deployed to a staging environment for further manual testing by QA engineers
- If manual testing passes, the change is released into production.
- The change is monitored using NewRelic, CloudWatch, and Loggly for any unusual change in metrics.
- If no issue is found, the ticket is closed and interested parties are notified

Logging

All network requests, user logins, employee logins, SSH login attempts, critical component changes, suspicious network traffic, port scanning, administrative actions, and application errors are logged. Alerts are also configured for anything considered critical or unusual with these logs e.g. a spike in SSH login attempts.

Security Evaluation

General security processes and methods are evaluated on a quarterly basis by the DevOps team.

PCI Compliance

RedShelf utilizes Stripe, specifically Stripe.js, as the payment processor for all transactions. RedShelf's integration with Stripe is such that when a customer enters their credit card information all of the data is sent directly to Stripe. RedShelf servers never touch or store the sensitive information. Furthermore, RedShelf will never be in possession of a customer's credit card number before, during, or after a transaction.

Given RedShelf's method of payment processing, RedShelf has decided to fully rely on the PCI DSS compliance achieved by Stripe. Stripe has achieved Level 1 PCI Compliance, the most stringent level of certification available. Stripe's Level 1 PCI compliance has been verified and audited by a PCI-certified auditor.

RedShelf Security Policy

Policy Overview & Purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data, customer data, partner data, and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When new hires receive company-issued equipment they will receive instructions for:

- Disk encryption setup
- Password management tool setup
- Installation of antivirus/ anti-malware software

They should follow instructions to protect their devices and refer to our Security Specialists if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can refer to our IT Specialist.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure, so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lowercase

letters, numbers and symbols) and avoid information that can be easily guessed (e.g.

birthdays.)

- Remember passwords instead of writing them down. If employees need to write their passwords down, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our Security Specialists for help.

- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.

- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

- Report scams, privacy breaches and hacking attempts

- Ensure all sensitive or critical data is encrypted at rest using methods provided by our IT Specialists

Our IT Specialists need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Specialists must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.

- Report stolen or damaged equipment as soon as possible to IT Department.

- Change all account passwords at once when a device is stolen.

- Report a perceived threat or possible security weakness in company systems.

- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.

- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy. Our Security Specialists should:

- Install firewalls, anti-malware software and access authentication systems.

- Arrange for security training to all employees.

- Inform employees regularly about new scam emails or viruses and ways to

combat them.

- Investigate security breaches thoroughly.

- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage them to seek advice from our Security Specialists.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.

- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.