DocuSource of North Carolina, LLC.

SECURITY PLAN DOCUMENT

September 2008 v2.3

Scope of Document

This document represents the commitment of management within DocuSource to incorporate a strategic plan for security within the three key areas of our operation: 1) physical security, 2) print production security, and 3) network security. Our goal is to provide industry-leading solutions for our internal purposes and for those customers requiring us to handle confidential information and data, up to and including personally identifiable information (PII) and moderate-risk data as defined by NIST 800-53. The Docusource Security Plan is the responsibility of the VP of Operations with monitoring by the IT Director and enforcement by the management team of DocuSource.

Physical Building Security Plan

The DocuSource facility is located at 2800 Slater Road in Morrisville, N. C. and is comprised of approximately 28,000 square feet of office, manufacturing and warehouse space. The building is protected by a fire alarm system that is monitored by BFPE 24 hours a day, 7 days a week.

Public Access

The building is open for normal business Monday thru Friday from 8:00am to 6:00pm. The main entrance doors at the front of the facility are the only public entrance to the building. During our normal hours of operation, this area is staffed by a minimum of two (2) customer service people and a maximum of six (6) team members. The customer service area houses a convex mirror so that all customer service representatives can view the front entrance without leaving their desks. The main entrance has automatic doors that only operate during normal business hours. The on/off switch for both sets of doors is inside our facility and can't be activated by anyone on the outside. We run a second production shift in the building and occasionally have customers come to our building after normal business hours. When customer entry is necessary, they call in advance to let us know they are coming and upon arrival use a call box located on the outside of the building next to the main entrance. The call box rings into our phone system and is answered by a DocuSource employee who lets them in the building. This access is monitored by our Facility Access Program to advise management of door usage outside of normal business hours.

Access for Staff & Support Staff

There are a total of four other entrances into the building: one rear fire exit not accessible from the outside, another rear exit and two side exits. The access for these doors is controlled and monitored by our Facility Access Program and supported by Tech Systems, an industry leader in physical building access security. Staff members are granted access based on permission levels and work schedules.

To facilitate the special requirements of customers, we offer secure rooms within our facility that can be used by our production staff to produce work or by our customers to review work. We offer both a card access secure room and a keyed access secured room.

Tours of our facility are always led by a management team member and are limited to specific general production areas. The building design includes a hallway with viewing windows that runs around our

production area. This design protects any confidential work in progress from being viewed by anyone on a tour. If the tour requires inspection of a specific area, confidential work is halted in that area and the work is moved or covered.

Training

Each new staff member is trained on the physical security plan within 30 days of hire. Quarterly reviews of our physical security plan and any approved updates are held with all staff members.

Print Document Security Plan

Our core business is the production of printed materials for our clients. These printed materials may contain confidential information and/or information that include moderate-risk data. Our goal is to provide print services manufactured in a secure environment so that the product delivered to our clients does not experience any security or confidentiality breach.

Personnel Screening & Confidentiality Agreements

As part of our hiring due diligence, all potential employees must pass pre-employment background checks, drug checks and screening which are all administered by certified agencies. The DocuSource management staff then reviews all of the results. If any red flags are spotted, the person is not hired. The next step of the hiring process is for each employee to review and sign a confidentiality agreement relating to vital information and trade secrets owned by DocuSource and/or its customers. This agreement is included in our Employee handbook. When any changes occur in our handbook, we meet with our staff to go over them. We also have quarterly employee meetings during which we explain the definition of confidential business information and the requirement of abiding by our non-disclosure/confidentiality agreements. We go over examples and outcomes of situations that have occurred in our industry to further explain the implications of not abiding by the agreement. We also explain that every confidentiality agreement that is signed by the company CEO represents everyone in the company. The policies and procedures that DocuSource has implemented protect the Confidentiality, Integrity and Availability of any ePHI (Electronic Protected Health Information) received from any CE (covered entity) for printing as required by the HIPAA Security Standards.

Print Production

Documents and printing waste for security sensitive documents and/or confidential documents is placed in secure shred bins. We have key vendor relationships to provide onsite shredding of confidential print waste as directed by our customers. If a customer wants us to return waste from his/her project, we accommodate that as well.

We employ print production workflows that are compliant with NIST 800-53 rv1 for handling 'moderate risk' data.

Limited team member involvement on projects can be arranged for projects requiring controlled access. Secure production rooms that are monitored by our Facility Access Program are also available as necessary.

During customer site visits, any production related to confidential documents is halted and/or removed from the facility tour path. The CEO, the Production Manager or the VP of Operations must pre-approve any customer tours to ensure that the confidential document rules are enforced at all times.

Training

Each new staff member is trained on the physical security plan within 30 days of hire. Quarterly reviews of our physical security plan and any approved updates are held with all staff members.

Network Security Plan (including Internet/Web)

DocuSource is partnered with Tripwire, an industry-leader in network security. Our servers, workstations, and desktop systems are constantly monitored by Tripwire Enterprise software which generates daily reporting of changes and security issues that are in-turn managed and corrected by our IT department. All internal computer systems are compliant with NIST 800-53 rv1 with specific network workflow meeting the 'moderate risk' criteria.

DocuSource uses a Windows 2003 Server platform system and has deployed a company-wide file security plan using Symantec products including, but not limited to, virus protection and software firewall protection. Data is not accessible from outside of our intranet since these servers reside behind a hardware firewall. Only those files requested by the customer are placed on servers open to the Internet (this is our Pronto Web Portal hosted by Pagepath Technologies). Access to company and customer files is controlled by access-rights available within Windows server software and audited by our Tripwire software.

DocuSource is a leading provider of on-demand digital printing and offers web-based services for customers to submit and access their files. We offer two distinct portals for ecommerce; 1) web-based portals thru our Pronto systems, and 2) FTP server software. All software is permissions-based. Access-rights are determined by the customer and the needs they have related to online ordering. Web-based ordering services can be secured with SSL technology (encryption) if requested by the customer. Our web-based portals are a SAS (software as a service) provided by Pagepath Technologies and feature industry-leading security as shown in the attached web-security document. Our FTP server is restricted to users who have been given a login and password. The usage of a login and password restricts each user to his/her personal folder on the server so no cross contamination of data can occur. No anonymous logins are allowed. Our Tripwire software monitors the FTP server.

Client documents that are kept on our server for reprinting are stored in an archive directory. Only administrators are allowed to add/delete/modify these documents. All production staff members have read-only access for reprinting purposes. All client documents are also backed up on a nightly basis to tape for recovery in the event of an emergency.

Backup recovery is an integral part of our security plan. DocuSource has two distinct backup programs for internal key data and customer data. The first backup system is a daily program rotation of tape backup. There is a complete set of backups tapes kept offsite as well as onsite. The second system is a rolling 31-day rotation of our active jobs system.

Our network security infrastructure is evaluated on a daily basis by Tripwire Enterprise and security failures are addressed within 48 hours. Customers will be notified by management of any security related breach within 24 hours of the occurrence.

This security document and plan will be monitored and adjusted on a quarterly basis or as necessary to meet the technological and physical needs of our business and customers' requirements. Implementation of any change will be documented and outlined in future amendments to our Security Plan. Any change to the Security Plan will be approved by three key staff members at DocuSource: 1) the IT Director, 2) the VP of Operations, and 3) the President and CEO.

Training

Each new staff member is trained on the physical security plan within 30 days of hire. Quarterly reviews of our physical security plan and any approved updates are held with all staff members.

Support Documention: Pagepath Technologies (Pronto Online Web Submission)

Document Web Portal Security Features

Using DocuSource for your Internet storefront is not only smart, but also better than the alternatives. As you would expect, areas related to the products and services you provide, information about your organization, etc. can be visited by the general public. However, access to the job management and control areas of your DocuSource system are NOT open to the public.

Site Access

Your customers sign in to access their job management, job history and proofing areas using:

- An e-mail address, and
- A password.

Job Access

After they sign in, the customer can only see THEIR job files, etc. They will NOT see other customer's information. Of course, you and your staff will have access to all your customer job records.

e-Commerce Security

DocuSource sites come with built-in SSL (Secure Socket Layer), 128 bit encryption to protect financial and other sensitive information as it is passed from the customer to you.

- Automatically used during sign in, and
- Used on orders requiring credit card data.

Login Security

To provide you with maximum control, your DocuSource storefront has three access levels for your customers and prospects and four access levels for you and your staff:

- IP Whitelist. Restrict access to your website to specific IP addresses.
  Allow only people from specified IP addresses to enter the site.
- Account Creation. Control whether visitors can create an account.
- CAPTCHA. Require CAPTCHA verification.
  A type of challenge-response test, often using an image of distorted letters or numbers, used in computing to determine whether the user is human.
- Password Length. Set minimum password lengths of 6 to 50 characters.
  Longer passwords are generally more secure.
- Password Case. Enforce mixed case passwords.
  "abc123" is different than "ABC123".
- Security Question. Passwords may be reset after successfully answering a self-set security question.
  This avoids having a forgotten password sent by email.

Nine Security Access Levels

To provide you with maximum control, your DocuSource storefront has three access levels for your customers and prospects and four access levels for you and your staff:

- Customers & Prospects:
  1. General Public have access to your informational home pages and any file transfer, quote request, and similar pages you may designate.
  2. Customers have access to any file transfer and order/job ticket pages you designate, and to their own job records.
  3. Approvers, with your permission, have access to their employees' (your customer) job records.
  4. Viewers, with your permission, have access to their employees' (your customer) job records.

- You & Your Staff:

1. Staff access permits one or more of your employees to enter and retrieve customer files.
2. Job Administrator access permits one or more of your employees to enter, retrieve, and delete customer files.
3. Site Administrator access permits one or more of your employees to enter, retrieve, and delete customer files, as well as alter the basic operation of the site including creating order forms, changing color schemes, control access levels, etc.
4. Site Administrator has the same abilities as the Owner, with one exception.
5. Owner has total control of the site.

File Encryption Security

Protecting customer files that are transferred to you is another built-in feature:

- The SimpleSend file transfer option can use a password you designate,
  - Automatically used to encrypt the files,
  - The encryption password is needed to open the files.
- The Windows PDF2U file transfer option can use https to automatically use RC4 128bit encryption during the file transfer.

Server Security

The servers are physically housed in PagePath's own, locked storage racks in a world-class facility protected by:

- Armed guards,
- Video surveillance,
- Biometric hand geometry reader access,
- "Man-trap" double door entrances,
- Automated site backup.
- New firewall technology that assures your data remains safe and secure.

Server Reliability

Recognizing that those seeking a Service Level Agreement (SLA) have concerns about service reliability, below is an overview of the steps we've taken to keep your data secure and downtime to an absolute minimum:

- Hosted within a leading international collocation facility featuring redundant Tier 1 Internet connections, N+1 redundant battery & diesel power, redundant HVAC and 24x7 on-site security & technical support.
- Our systems include additional redundancies to mitigate any single point of failure from negatively affecting your operations.
- International automated monitoring system that will alert our administrators within 5 minutes of a service outage on a 24x7 basis.
- After hours system maintenance and application upgrades with posted notices.

All of these steps have provided us with an historical uptime greater than 99% over the last 2 years.

Security Plan Authorization Statement

This security plan **version 2.3** is hereby drafted and approved for public release on September 29, 2008.

Rob Montgomery – IT Director

Derek Dorroh – Vice-President of Operations

Kathy D. Murchison – President & CEO