White Paper

Improved Delivery and Management of Critical Information:

Corporate Organisations

Author : Ben Martin

Document Number : WHP-1006

Revision : V5.6

Issue Date : January 2015

Safe4 Information Management Limited

1 Kingsmill Park
London Road
Loudwater
Buckinghamshire
HP10 9UB
United Kingdom

☎ +44 845 094 8045
@ enquiries@safe-4.co.uk
www.safe-4.co.uk

Safe4 Information Management (Africa) (Pty) Ltd

Building No 2, Pinewood Office Park
33 Riley Road
Woodmead
Johannesburg
PO Box 555
Strathavon 2031
South Africa

☎ +27 11 234 2563
www.safe-4.co.za

Contents:

1. What is meant by Critical Information?

In the course of conducting everyday business operations, many different organisations provide the end-product of their service in the form of a document. Information produced in this way has value to the recipient of the service being provided; it is normally required for regulatory or compliance purposes, and indeed may be required by the recipient in the conduct of their own business.

For the purposes of this White Paper, Critical Information is regarded as anything which is expressed in document form as the culmination of a service for which charges have been made or significant effort has been invested, and which therefore has value in and of itself. The concept also applies to information which is being retained as a record - of a transaction, a process of communication, or an event for which documentary evidence may be required in the future. If lost or misplaced, some degree of cost, inconvenience or delay will result. There is therefore a need to safeguard it through the process of storage, and if appropriate the process of delivery to the recipient, and for it to be permanently available to authorised parties after delivery.

An enormous range of organisations deliver Critical Information to a wide variety of recipients. This paper will deal specifically with situations which involve corporate organisations providing documents to employees or agents, external contractors, and internal parties to handle scenarios such as project management, human resources management, general records management or disaster recovery.

2. Who is this White Paper aimed at?

Corporate organisations who deliver documents to employees, agents, contractors, or specific internal parties

Virtually all corporate organisations in today's business environment have made substantial investments in IT infrastructure. This infrastructure will support the entire business model, from design and manufacture of physical products, to distribution, sales, finance, marketing, health and safety, and business planning. Such systems capture and manage the corporate intellectual capital of an organisation, and are generally architected on sophisticated platforms and protected by extensive security and disaster recovery measures.

The purpose of this White Paper is to explore those areas of business which are not accommodated by internal IT systems. In such cases, documents are delivered to internal and external parties, but the requirements of information management good practice and corporate governance do not necessarily stop when a document leaves the business.

Examples of such situations are:

i. **Employees**

Employees of corporate organisations will receive many documents during the course of their employment, including letters of appointment, contracts of employment with occasional variations, annual reviews and assessments, disciplinary measures, corporate updates and information, and many others. The onus on the organisation to provide such information is addressed when the document is delivered, but the way in which that document is managed and stored by the individual after delivery can impact the employer, particularly if delivery is disputed.

ii. **Agents or consultants**

A similar situation exists with agents or consultants who are appointed for a limited duration, but for a specified task. Whilst there may be no contract of employment as such, the organisation has many obligations covering the agent or consultant's engagement with the company.

iii. **External contractors**

Contractors are frequently required to enter an organisation's premises and carry out specified tasks, often interacting with members of the organisation's staff. Relying on physical delivery of hard copy documents can expose the organisation to a number of risks. Health and safety concerns are often paramount in such situations.

iv. **Share option schemes**

Many corporate organisations, both large and small, offer their employees participation in share option schemes. Such schemes require the delivery of a significant volume of documents, many of which will be updated or altered over time, and many may be required after the employee's engagement with the company has ended.

v. **Disaster recovery plans**

All well-managed corporate organisations will have disaster recovery arrangements in place to handle the results of catastrophic events that may make IT systems and services unavailable. Transfer of operations to a DR site is normally handled through a carefully-planned process, often by specialised third party companies. However, the disaster recovery plan, which is often a large and complex document that will normally be subject to constant change, will probably be held in paper form, or on a series of personal computer hard discs. It may thus not be readily available when a disaster occurs. Corporate managers will need to make key decisions and undertake specific actions immediately such situations occur: how to communicate with the media, how to communicate with staff, how to manage pressing financial requirements, how to handle customers and suppliers. Guaranteed immediate access to the plan by all authorised officers will greatly facilitate a successful recovery from any catastrophic occurrence.

vi. **Managing projects**

Corporate project managers will have to interact with many different parties, both internal and external. All of the life-cycle phases of a project are dealt with in document form, and immediate successful delivery to all participants - both internal and external - is essential for effective project execution. It may also be necessary on some occasions to be able to prove that documents were provided correctly, and that they have been received and accessed by recipients.

vii. **Dealing with the media and external marketing agencies**

Before marketing or financial information can be released to external agencies or the media, it will be subject to revision and editing internally. The completed version will then be issued, often by email, to selected recipients.

viii. **Board papers and agendas**

Sharing highly confidential information regarding matters dealt with at board meetings can often involve the use of insecure communication methods - email, hard copy etc. Such information needs to be protected at all times from unauthorised access.

Although this list is not exhaustive, it illustrates the wide range of different information types that may not necessarily be addressed by current internal IT resources. Some of these address requirements for good practice and service to employees and agents, others deal directly with business continuity under difficult circumstances.

3. Methods of delivering documents to recipients

Traditionally, corporate organisations have used well-known means of delivery for the critical documents that they send to recipients, both internal and external. The most familiar are:

- Hard-copy post
- Hard-copy courier services
- Email
- Electronic media such as CDs or memory sticks
- DX for professional practitioners

Each of these creates its own set of difficulties. In essence, traditional methods of document delivery and storage suffer from some distinct disadvantages:

- Cost
- Inconvenience
- Delays
- Lack of security and confidentiality
- Risk of accidental loss or theft of corporate information, with huge regulatory repercussions and potential reputational damage
- Difficult to create an audit trail of secure delivery and usage
- Administrative effort replacing documents which have been misplaced by internal or external recipients
- Administrative effort in locating misfiled documents; industry surveys show that even in well-run organisations traditional storage methods can result in up to 30% of information being misfiled and therefore not retrievable
- Damage to the environment through consumption of paper and printing resources, and physical transportation of hard copy information

Upon receipt, each recipient will have to store the documents in a way which allows rapid retrieval and use of the information. Even the best-organised of recipients will have occasional difficulty in finding information, and the worst-organised will often be completely unable to locate important documents when they are most needed.

4. How can the situation be improved?

Safe4 Information Management conducted extensive research into the requirements for improvements in delivery of critical documents to various recipients by corporate organisations. A number of internet-based systems for storage of computer files are available, and these provide a useful service. However, they have generally been designed for use by the consumer, and are not directed explicitly towards the solution of a clear business problem:

How can corporate organisations get documents to specific types of recipient quickly, safely, securely, and at lower cost?

Safe4 is a web-based service that has been designed from first principles to assist corporate organisations to offer the most efficient and secure means possible of getting documents to a variety of types of recipient, and at the same time ensure that the recipient enjoys immediate and confidential access to their stored information. In doing so it not only adds value to the relationship with the recipient, but it helps to achieve significant reductions in internal administrative and delivery costs.

The design brief for ***Safe4*** was based on some mandatory requirements:

- Provision of a secure vault, hosted on the Internet, and available 24/7 from anywhere
- Banking-level security for control of access to the system, based on username, password and PIN
- Secure encryption of files as they are lodged in the vault
- Multi-user capability, so that service provider and client can see the ***same file*** from different viewpoints
- Automatic email notification of new files being placed into the system
- Audit trail of document delivery and access
- Versioning, to allow life-cycles of a document to be managed
- A flexible and open architecture, to allow the system to be integrated directly with the corporate organisation's (or recipient's) line-of-business systems if necessary
- Complete independence from the corporate organisation's or recipient's own IT systems and domain

In the development of the ***Safe4*** service, the efficiency of document delivery was given the highest priority. Hence the ability of the system to replace many of the traditional methods used to get documents to recipients, and provide significant benefits to document creators and consumers alike.

5. What does *Safe4* do?

Safe4 offers the capability for any organisation to deliver documents securely to a client or any other party, instantly over the internet into a document vault that only the providing organisation and its designated recipients can access, and allow permanent subsequent access to such documents without compromising the organisation's mission critical systems and databases. It enhances communication, reduces cost and improves security, as well as radically reducing carbon emissions. The ***Safe4*** vault automatically notifies the recipient when a document has been delivered and is available for them to download or view.

The document is stored securely within a folder structure that the provider can define, similar to Windows Explorer, and which is fully backed up and always accessible over secure internet connections for authorised users only.

The recipient can access the document directly through the ***Safe4*** secure gateway on the Internet. Banking standard protection of Username, Password and PIN applies, and all accesses are logged for audit and reporting purposes. Importantly, the recipient does not need to have access to the provider's business applications.

In summary, the functions provided by ***Safe4*** can broken down into separate sections:

5.1 Unique and flexible architecture

- Multi-tenanted structure
- Unlimited number of providers
- Each provider may create an unlimited number of vaults, for external or internal applications
- Each provider may have an unlimited number of users
- Each vault may have an unlimited number of users
- Each user may be connected to multiple provider accounts
- Each user may be connected to multiple vaults
- Users may have a combination of different provider and vault account connections through a single login

5.2 Provider account branding

- Each provider account can feature a different logo, and can be named according to the application in question (for example a law firm may wish to brand corporate and private client accounts differently)
- Provider accounts can use different terminology to describe vaults (for example Clients, Projects, Matters, Data Rooms, etc)
- Provider accounts can have customised individual welcome text for the login page, and disclaimer text for user invitation emails
- Vaults within each provider account can carry a link to the provider's website

5.3 User management

- Both provider and vault users are invited by email to register for the system
- Users can add new invitations to their existing accounts
- Permissions and membership of security groups can be determined at the time of the invitation, or at any time subsequently
- Users can be disabled instantly; disabled users will lose their access to the system immediately
- If the use of a PIN is not enforced by the administrator, individual users can choose to set up their own PIN

5.4 Security groups

- Security groups are applied to folders and to users; this will determine the actions that each can perform on the contents of a folder
- Users can be permitted to upload, move, rename and delete files
- Users can also be permitted to upload, move, rename and delete folders
- It is thus possible for users to be permitted to upload files, but not move, rename or delete them
- Sub-folders can be given different security groups from their parent, thus allowing more restrictive control of sub-folders

5.5 Permissions

- Provider users can be permitted to manage both provider and client users, as well as to allocate security groups to users and folders
- The ability to manage branding can be applied selectively to provider users, as can the ability to set up the web link from the files and folders page
- ***Safe4*** has a comprehensive reporting capability. Access to this is also controlled by a permission setting
- Content control through the scanning of uploaded files for protective markings is also a function that is permission-controlled

5.6 Uploading files

- Files can be uploaded using the web interface into specific folders, in quantities of up to 20 at a time
- Files of up to 470 mb have been successfully uploaded to ***Safe4***. The maximum file size will be governed by the speed of the internet connection available
- Comments can be added to files as they are uploaded, for example to explain why a new version of a file is being uploaded
- Email notifications of file uploads can optionally be triggered automatically. These emails contain a link to allow the recipient to login and view the files. The files themselves are never carried by email
- Multiple versions of files can be uploaded into ***Safe4*** and managed in a single view within a folder; previous versions can be displayed if required

5.7 Downloading files

- Files can be opened for viewing; image files are viewed in a new browser tab, files with editable content such as MS Office documents will be opened using the mother application
- Multiple files can be downloaded in a single action, and placed in a ZIP file on the user's computer
- When using the web interface, files held in ***Safe4*** cannot be edited. To change the contents of a file, the file must be edited locally and uploaded as a new version
- Using the WebDAV interface, described below, editable files can be edited online, with the modified version being held by ***Safe4*** as a new version

5.8 Folder management

- Folder structures can be created to reflect the provider's business, and the nature of the information being stored
- Users can be granted the ability to create, move, rename and delete folders
- No limit on the number of folders, nor on the number of sub-folder levels
- The root folder can be renamed by the provider administrator
- Common Folders are visible to users of all of the vaults in a provider account. This allows certain types of document to be made available to a large population of users by a single upload action
- Vaults cab copied very rapidly; this function can carry across the complete folder structure, including permissions, to the new vault

5.9 *Safe4* reporting and file history

- Reports on activity within ***Safe4*** can be generated by authorised provider users
- Any date range can be selected, as can any of the provider accounts and vaults accessible to the user in question
- Every single function available within ***Safe4*** can be queried in this way
- All actions performed on the files within ***Safe4*** are recorded and made available as an audit trail. This is shown adjacent to the file in question, and does not require a report to be run

5.10 WebDAV

- Web Distributed Auditing and Versioning has been implemented within ***Safe4***
- This allows a network drive to be mapped on Windows and Apple computers, connecting to ***Safe4*** in the cloud
- All of the provider accounts and vaults that the user is permitted to see will be displayed as folders and sub-folders in Windows Explorer
- All of the functions available in Windows can thus be used: files can be uploaded and downloaded by simple dragging and dropping them between folders in Windows
- New files can be created in applications such as Microsoft Office, for example, by right-clicking and selecting "New ..."
- MS Office files can be opened, edited, and saved simply by double-clicking in the normal way. The amended version is placed into ***Safe4*** as a new version of the original file. Previous versions can then be displayed in the web interface if required

6. What benefits does *Safe4* provide for the service provider?

The implementation of the ***Safe4*** service as an extension of a corporate organisation's business will achieve significant advantages:

- More efficient and secure document delivery, with immediate access for recipients
- Evidence of document delivery, and of documents being opened by a recipient
- The ability to share documents confidentially with external third parties, such as a solicitor, accountant or contractor for negotiation and review
- No hardware or software to procure or maintain
- Very low-risk, with no start-up costs other than those associated with data-uploading and integration into business processes
- Pure "Software-as-a-Service", with delivery across the Internet, meaning that the corporate provider and the recipient have no hardware or software to upgrade through releases of new versions and system enhancements
- No need to open up the corporate provider's own IT systems to external client access, thus avoiding the cost, risk, and implementation challenges associated with such an approach
- Very high levels of security
- Value-added service for the corporate provider, potentially with improved quality of service
- Rapid provision of information to many recipients in a single action by using the ***Safe4*** Common Folders facility
- Opportunity for an annually-recurring revenue stream for the corporate provider if appropriate
- Competitive differentiator in the marketplace to assist the provider to leverage the procuring of new business against competitors
- Built-in disaster recovery for all externally-facing files
- No administration or management worries for the corporate provider – everything is handled by Safe4 Information Management
- Support for environmental sustainability – lowering carbon emissions and reducing the use of scarce resources

The unique structure of ***Safe4*** allows the provider to share information with the recipient as well as other third parties, depending on the nature of the relationship. In all cases, ***Safe4*** can offer a storage model which makes specified information available to certain parties and not others, thus protecting confidentiality and maintaining regulatory compliance.

7. How does *Safe4 h*elp the recipient?

As well as the benefits listed above for the corporate provider, ***Safe4*** assists the recipient in a number of ways:

- Very simple to use, with comprehensive help
- Immediate access to documents provided by the organisation
- Complete confidentiality
- Access 24/7, from any device with Internet access
- The ability to upload their own private documents to ***Safe4***, depending on the level of access granted by the corporate organisation
- The ability to use and share a secure and confidential document store without the need to set up a network domain or virtual private network
- No need to worry about backup; this is completely taken care of by ***Safe4***

8. Security

Safe4 has been architected using state-of-the-art technology components and development methods. This ensures that the service provider and the recipient are able to gain the benefit of an application which is constantly being optimised for performance and efficiency, and which is being seamlessly upgraded without any disruption to the individual user.

The highest possible levels of security are the key objectives of ***Safe4***. With the regular emergence of new internet security threats, it is vital that ***Safe4*** users can be sure that their data is being handled in the safest way possible.

Using independent testing services, Safe4 has been assessed among the top 0.8% most secure sites on the internet, out of more than 1.2 million tested.

Safe4 regularly undergoes independent penetration testing, and has emerged with excellent ratings for security. This service is undertaken in accordance with the UK Government's IT CHECK scheme, administered by GCHQ.

The key security features of the service are:

i. **HTTPS connection**

Security starts with the connection between the user's browser and the ***Safe4*** servers which is secured using TLS (Transport Layer Security, the successor to SSL). Configuration of TLS is complex and a surprising number of websites are badly configured compromising their security. ***Safe4*** is configured to the highest standards and is rated "A+" in independent testing. This places ***Safe4*** in the top 0.8% of more than 1.2 million web sites that have been assessed.

ii. **Encryption at rest**

Files that have been uploaded are encrypted using AES-256 before being saved to storage. When a file is downloaded it is checked to ensure that it is exactly the same as the file that was uploaded and has not been tampered with.

Safe4 does not support searching inside of files that have been uploaded. This is because the indexes cannot be encrypted and if compromised the content of the documents would be accessible.

iii. **PIN protection**

An extra layer of protection can be added by requiring users to set a PIN in order to access their vault using an on screen keyboard to defeat key loggers. This gives a similar level of protection to one time passwords, or text codes – without the inconvenience.

iv. **Virus protection**

All files that are uploaded are checked for virus infections. This helps to ensure that ***Safe4*** does not pass an infected file onto a third party, damaging the provider's reputation.

v. **Enforce information security policies**

Safe4 provides support for the provider's information security policies. Whitelisting enables control of the individual types of files that can be uploaded – for example enforcing the upload of PDFs only to ensure that modifiable content is never uploaded. Where more stringent requirements are needed ***Safe4*** provides support for validating protective markings, and rejecting files with altered extensions and password-protected files.

vi. **Permissions**

Safe4 implements comprehensive security permissions which enable the provider to apply fine grained control over access to individual parts of the system.

vii. **Hosting**

Safe4 is hosted by a world leading hosting partner - Rackspace - at data centres based in the UK. Rackspace also give security the utmost priority and are fully ISO27001 certified. See their website for more details.

End of Document

If you have any comments on this document, or if you would like to discuss any of its contents with *Safe4*, please visit our website:

- **Articles:** http://safe-4.co.uk/blog/
- **Contact:** http://safe-4.co.uk/contact/

www.safe-4.co.uk
ben.martin@safe-4.co.uk