Guidelines for Uploading Documents in *StanReady*

StanReady allows you to upload documents that may be useful in recovering and continuing your department's Critical Functions. Following a disaster, you may not have access to your office and/or your computer. However, *StanReady* includes documents that have been uploaded, which can be accessed from off-campus.

Documents uploaded in *StanReady* are copied to a secure server, for access by authorized users only. Individuals with access to your plan will also have access to your uploaded documents.

Examples of Documents to Consider Uploading

The following list describes documents that may be useful to your business continuity plan in *StanReady*.

If a document is maintained in a document management system (e.g. SharePoint or Knowledge Link), please consult the document owner before uploading in *StanReady*.

□ Documented Business Processes
- Desktop manuals
- Written instructions

□ Specifications, Drawings, Inventory
- Specs on specialized equipment that may be needed for expedited replacement (e.g. receipts, purchase orders, photos)
- Description of inventory
- Hardware inventories
- Building plans/drawings

□ Blank Forms
- Forms needed to resume your Critical Functions (remember, you may not have access to your office or to the campus website)
- Order forms

□ Contact Information
- Employees
- Vendors
- Donors

□ Important Legal Documents
- Contracts
- Lease Agreements
- Service Agreements

□ Research Files

□ Policy Manuals
- Policies
- Procedures
- Guidelines
- Standards

Confidential Documents

StanReady site is secure in uploading documents via SSL so encrypting individual documents isn't necessary; however, some documents that are extremely confidential should not be uploaded.

The following list contains examples of confidential documents that should not be uploaded in *StanReady*:

□ **Personal Information Data**
- Passwords or credentials
- PINs (Personal Identification Numbers)

- Birth date combined with last four digits of SSN and name
- Tax ID with name
- Driver's license, state identification card, and other forms of national or international identification (e.g. passports and visas) in combination with name
- Social Security number and name
- Biometric information

□ **Financial Information**

- Credit card numbers with cardholder name
- Bank account or debit card information

□ **Health Information**

- Medical reports related to an individual
- Health insurance information related to an individual
- Psychological counseling records related to an individual

□ **Primary Account Number (PAN) (credit card number) AND any of the following if stored, processed, or transmitted with the PAN:**

- Cardholder Name
- Service Code
- Expiration Date

□ **Technical Security Information**

- Vulnerability/security information related to campus or computer information system
- Root passwords for your server
- Software license keys
- /etc/password, /etc/shadow, other /etc/* files

□ **Law Enforcement Information**

- Law enforcement records related to an individual