DATA CLASSIFICATION MATRIX GUIDELINES

	NON-SENSITIVE		SENSITIVE	
	NON-CONTROLLED	**CONTROLLED**	**CRITICAL INFORMATION**	**RESTRICTED INFORMATION**
EXAMPLES	Brochures, news releases, Customer information	Routine correspondence, employee newsletter, internal phone directories, in-office memoranda, internal policies, processes, guidelines, and procedures	Division financial data, purchasing information, vendor contracts, risk assessments, and internal auditing reports and findings.	Statutorily protected and sensitive information, and corporate information such as customer forms, corporate forms, strategic corporate plans/ financial information, employee records, employee health information, and investigation reports and finding.
CRITERIA	Information, which can be made available to anyone without exception. It is neither sensitive nor controlled.	Information which management believes requires limitations on internal access on a "need-to-know" basis, but which does not fall under the definition of "sensitive information".	Information, which must be available in order for [ORGANIZATION] to effectively perform its mission and meet legally, assigned responsibilities. Critical information requires that special precautions be taken to ensure its accuracy, relevance, timeliness, and completeness. This information, if lost, could cause significant financial loss, inconvenience, or delay in performance of [ORGANIZATION] mission and a loss of public trust.	Restricted mandatory information is any information that has limitations placed upon its internal access and that may be disclosed only in accordance with an executive order, public law, federal statute (HIPAA, GBL, Privacy Act of 1974, etc.), and supporting, and [ORGANIZATION] policies, guidelines, procedures, and processes.
HANDLING STANDARDS	No Special handling required.		Encryption is required when sending information over an untrusted network i.e., the Internet or non-secure email system. When sensitive information is commingled with non-sensitive information through computer processing and merging of data or insertion of documents files, the resulting file, tape, or disk which contains the commingled data must be clearly labeled that "Sensitive information is Included..	
1. RELEASE TO THIRD PARTIES STANDARDS	Available to the general public and for distribution outside of the [ORGANIZATION].	Intended for use only within the [ORGANIZATION]. May be shared outside the [ORGANIZATION] only if there is a legitimate business need to know, and is approved by the data owner and users manager.	Access limited to as few persons as possible on a need to know basis. Information is very sensitive and closely monitored using auditing tools. Information is controlled from creation or acceptance to destruction or return of information. Release only permitted by appropriate policies and procedures.	

	NON-SENSITIVE		SENSITIVE	
	NON-CONTROLLED	CONTROLLED	CRITICAL INFORMTION	RESTRICTED INFORMATION
2. **TRANSMISSION BY**POST, FAX, E-MAIL STANDARDS				
a. Mail within the organization (interoffice).	a. No special handling required.	a. No special handling required.	a. Sealed inter-office envelope marked and labeled “sensitive Information”. Notify recipient in advance.	
b. Mail outside of the organization	b. No special handling required.	b. 1st class mail. No special handling required.	b. 1st class USPS mail. Trackable delivery required, *e.g.* messenger, FedEx, U.S. express, USPS certified, or return receipt mail.	
c. E-mail within the organization	c. No special handling required.	c. No special handling required.	c. Refrain from use of customer SSAN. Use of e-mail strongly discourage unless encrypted.	
d. E-mail outside of the organization	d. No special handling required.	d. No special handling required.	d. Use of customer SSAN prohibited, unless encrypted or emergency situation. Use of e-mail strongly discouraged.	
e. FAX				
1). Location of fax machine.	1). Located in area not accessible to general public.	1). Located in area not accessible to general public.	1). Located in area not accessible to general public and unauthorized persons.	
2). Use of fax coversheet.	2). Required.	2). Required.	2). Required. Coversheet labeled “Sensitive Information”.	
3). Transmission safeguards.	3). Reasonable care in dialing.	3). Reasonable care in dialing.	3). Telephone notification prior to transmission and subsequent telephone confirmation of receipt required.	

	NON-SENSITIVE		SENSITIVE	
	NON-CONTROLLED	**CONTROLLED**	**CRITICAL INFORMATION**	**RESTRICTED INFORMATION**
3. TRANSMISSION BY SPOKEN WORD STANDARDS a. Conversation/ Meetings b. Telephone c. Cellular Telephone d. Lobby announcement e. Overhead pages	No special precautions required.	Reasonable precautions to prevent inadvertent disclosure.	Active measures and close control to limit information to as few persons as possible. a. Enclosed meeting area. Public areas prohibited. b. Avoid proximity to unauthorized listeners. Speakerphone in enclosed area. Use generally discouraged. c. Use of digital telephones discouraged, landline preferred. d. Lobby announcements. e. No overhead pages.	
4. **PRINT, FILM, FICHE, VIDEO STANDARDS** a. Printed Materials b. Sign-in sheets/Sign-in Logs c. Monitors/Computer Screens	No special precautions required.	Reasonable precautions to prevent inadvertent disclosure. a. Store out of sight of non-employees. b. Placement out of sight of non-employees. c. Positioned or shielded to prevent viewing by non-employees.	Active measurers and close control to limit information to as few persons as possible. a. Store out of sight in a lockable enclosure. b. Subsequent signers cannot identify signer. c. Position or shield to prevent viewing by unauthorized parties. Possible measurers include, physical location in secure area, positioning of screen, use of password screen saver, etc.	
5. **COPYING STANDARDS**	No special precautions.	No special precautions.	Photocopying with approval by Data Owner. (Note: If a digital copier is used, cache needs to be erased.)	

	NON-SENSITIVE		SENSITIVE	
	NON-CONTROLLED	CONTROLLED	CRITICAL INFORMATION	RESTRICTED INFORMATION
6. STORAGE STANDARDS				
a. Printed Material	a. No special precautions required.	a. Reasonable precautions to prevent access by non-employees.	a. Storage in a lockable enclosure.	
b. Electronic documents	b. Storage on all drives.	b. Storage on all drives.	b. Storage on secure drives only. Password protection of document preferred. Use of Object Reuse to erase sensitive information or destruction of drive.	
c. E-mail	c. No special precautions required.	c. Reasonable precautions to prevent access by unauthorized personnel.	c. Encrypted storage and backup tape in a secure place or container.	
7. DESTRUCTION STANDARDS				
a. Destruction	a. No special precautions required.		a. Destroy in a manner that protects sensitive information.	
b. Location of waste paper bins.	b. No special Precautions required.		b. Secure area not accessible to unauthorized persons.	
c. Paper recycling.	c. Permitted.		c. Prohibited. Destruction or shredding required.	
d. Magnetic media/diskettes.	d. No special precautions required.		d. Use object reuse to overwrite sensitive information.	

	NON-SENSITIVE		SENSITIVE	
	NON-CONTROLLED	**CONTROLLED**	**CRITICAL INFORMATION**	**RESTRICTED INFORMATION**
8. PHYSICAL SECURITY STANDARDS				
a. Computer/Work-stations	a. Password screen-saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work.		a. Do not leave data unattended. Sign-off or power-off workstation or terminals not in use or leaving work area.	
b. Printing Documents	b. No special precautions required.		b. Printing of documents when necessary must not be left unattended. The person attending the printer must be authorized to examine the sensitive information being printed.	
c. Office Access	c. No special precautions required.		c. Access to areas containing sensitive information should be physical restricted. Sensitive information must be locked when left in an unattended room.	
d. Laptop, Palm, etc.	d. No special Precautions required.		d. Computer must not be left unattended at any time unless the sensitive information is encrypted or the hardware is secured in a locked file cabinet, room, or safe.	
9. ACCESS CONTROL STANDARDS	Available to the general public.	Generally available to all authorized users on a need to know basis.	Must have a business need to know the information. Must have written approval of the data owner.	
10. AUDIT STANDARDS	None	None	Access shall be granted by the data owner and audited.	