OYA Information Handling Guidelines

	Level 2 - Limited	Level 3 - Restricted	Level 4 - Critical
Transmission by mail, facsimile, e-mail			
Interoffice Mail	No special handling required.	Inter-office or regular envelope marked and labeled "Restricted Information."	Sealed envelope marked and labeled "Critical Information."
Mail Outside the Agency	No special handling required.	Transport using tamper-evident packaging and signature tracked	Transport using tamper-evident packaging and signature tracked
E-mail Within the Agency	No special handling required.	Recipient(s) are authorized to view the information.	Use of information prohibited, unless encrypted or emergency situation. Use of e-mail strongly discouraged. Recipient(s) must be authorized to view the information.
		The body of the e-mail must contain a label indicating the message may contain Restricted Information.	
		CJIS and SSA information - e-mail must be encrypted.	The body of the e-mail must contain a label indicating the message may contain CRITICAL Information.
E-mail Going Outside the Agency	No special handling required.	Recipient(s) are authorized to view the information.	Use of information prohibited, unless encrypted or emergency situation. Use of e-mail strongly discouraged. Recipient(s) must be authorized to view the information.
		The body of the e-mail must contain a label indicating the message may contain Restricted Information.	The body of the e-mail must contain a label indicating the message may contain Critical Information.
		Subject line must indicate "Restricted" at the beginning of the subject. Must use encryption service to encrypt e-mail.	Subject line must indicate "Critical" at the beginning of the subject. Must use encryption service to encrypt the e-mail.
		CJIS and SSA information - e-mail must be encrypted.	
Fax Transmission	Reasonable care in dialing.	When sending mental/physical health information or personally identifiable information (employee or youth records), telephone or e-mail confirmation of receipt.	Prohibited.
Fax Coversheet	Required.	Required.	N/A
Storage			
Printed Material	Reasonable precautions to prevent access by non-employees.	Storage in locked cabinet, drawer, or secured (locked) room when not in use.	Two layers of physical security such as within an access controlled building **and** stored in a lockable enclosure (cabinet, safe, etc).
Electronic Documents	Reasonable precautions to prevent access by non-employees.	Personally identifiable information (employee or youth records) must be stored on network file system. Access is controlled by information owner.	Information must be stored on network file system. Access is controlled by information owner.
		Access is limited to as few persons as possible on a need-to-know basis.	Access is limited to as few persons as possible on a need-to-know basis.

OYA Information Handling Guidelines

	Level 2 - Limited	Level 3 - Restricted	Level 4 - Critical
		Backup tapes are encrypted.	Backup tapes are encrypted.
E-mail	Reasonable precautions to prevent access by unauthorized personnel.	Personally identifiable information (employee or youth records) must be stored on network file system. Access is controlled by information owner.	Personally identifiable information (employee or youth records) must be stored on network file system. Access is controlled by information owner.
		Access is limited to as few persons as possible on a “need to know basis.”	Access is limited to "named" persons on a “need to know basis.”
		Backup tapes are encrypted.	Backup tapes are encrypted.
Destruction			
Location of Recycling Paper Bins	No special precautions required.	Area not accessible to unauthorized persons.	Area not accessible to unauthorized persons.
Paper Recycling	Place materials in locking recycle bins. Destruction or shredding is required.	Place materials in locked recycle bins. Destruction or shredding is required.	Place materials in locking recycle bins. Destruction or shredding is required.
		CJIS and SSA information: OYA staff must shred, not place in locked recycling bin.	
Mobile Data Storage Devices (e.g. floppy diskettes, CDs, DVDs, laptops, smart phones, USB flash drives)	Information Systems staff will destroy in a manner that protects information.	Information Systems staff will destroy in a manner that protects restricted information.	Information Systems staff will destroy in a manner that protects critical information.
Physical Security			
Computer / Workstations	Position or shield screen to prevent viewing by unauthorized	Position or shield screen to prevent viewing by unauthorized parties.	Position or shield screen to prevent viewing by unauthorized parties.
	Use of password screensaver.	Use of password screensaver.	Use of password screen saver.
	Lock workstation, logoff, or shutdown/restart when leaving work area.	Lock workstation, logoff, or shutdown/restart when leaving work area.	Lock workstation, logoff, or shutdown/restart when leaving work area.
Servers	Physical access to servers restricted.	Physical access to servers restricted.	Physical access to servers restricted.
	Access is limited to as few persons as possible on a “need to know basis.”	Access is limited to as few persons as possible on a “need to know basis.”	Access is limited to as few persons as possible on a “need to know basis.”
Printing	No special precautions required.	Documents must be retrieved as soon as possible and not be left unattended after business hours.	Documents must be retrieved as soon as possible and not be left unattended unless in a secured area.
Area Access	No special precautions required.	Access to areas containing restricted information must be controlled.	Access to areas containing critical information should be controlled.
		Information should not be readily viewable when left in an unattended room.	Information must be locked when left in an unattended room.

OYA Information Handling Guidelines

	Level 2 - Limited	Level 3 - Restricted	Level 4 - Critical
Mobile Data Storage Devices (e.g., floppy diskettes, CDs, DVDs, laptops, smart phones, USB flash drives)	Reasonable precautions to prevent unauthorized access, loss, or theft.	Reasonable precautions to prevent unauthorized access, loss, or theft.	Reasonable precautions to prevent unauthorized access, loss, or theft.
		Store device in locked drawer, cabinet, or room.	Store device in locked drawer, cabinet, or room.
	Store device in locked drawer, cabinet, or room.	Information must be encrypted or password protected.	Information must be encrypted and password protected.
Access Control	Generally available to all authorized users on a need to know basis.	Information Owner ensures adequate measures and controls are in place to limit access to as few persons as possible.	Information Owner ensures adequate measures and controls are in place to limit access to "named" persons on a “need to know basis.”
Access Review	No special precautions required.	Access granted by the information owner.	Access granted by the information owner.
		Perform periodic review.	Perform periodic review.
Hardcopy	Reasonable precautions to prevent inadvertent disclosure.	Information Owner ensures adequate measures and controls are in place to limit information to as few persons as possible.	Information Owner ensures adequate measures and controls are in place to limit information to "named" persons on a “need to know basis.”
Copying	Reasonable precautions to prevent inadvertent disclosure.	Approval from information owner.	Approval from information owner.
		Reasonable precautions to prevent inadvertent disclosure.	Reasonable precautions to prevent inadvertent disclosure.
Transportation	No special precautions.	Personal identifiable information (youth or employee records) must be transported in an enclosed container (pouch, folder, safe, etc.).	Information Owner ensures adequate measures and controls are in place to limit information to "named" persons on a “need to know basis.”
		Only authorized staff may transport. Staff will maintain physical control of the asset throughout the transport and ensure protection from view by unauthorized people. If the asset must be left unattended in a vehicle, the vehicle must be locked and the asset must be out of plain sight.	Only authorized staff may transport. Asset must be transported in an enclosed container (pouch, folder, safe, etc.). Staff must maintain physical control of the asset throughout the transport and ensure protection from view by unauthorized people. If the asset must be left unattended in a vehicle, the vehicle must be locked and the asset must be out of plain sight.