Information Security Approval Matrix

[ISAM] OHECC 2023



Presenters

Tony Kinne - Information Security Analyst (9yrs) - kinnema@miamioh.edu

Jake Harrison - Information Security Analyst (3yrs) - harrisjd@miamioh.edu



Session outcomes

- Awareness of a convenient and simple tool
- The value of a university approval matrix
- How to use it, periodic reviews, upkeep
- How to tailor the ISAM for your own use



applications files provision calendars disable delegate playback eveallow redactview rwardinvestigatevideo networks enable remove deprovision phones door



A need, indeed

- Requirements
- Compliance
- Equity and consistency
- Leadership support and awareness
- This is one model



Disclaimer

Different institutions may have varied policies and models when it comes to information security involvement in incidents and investigations



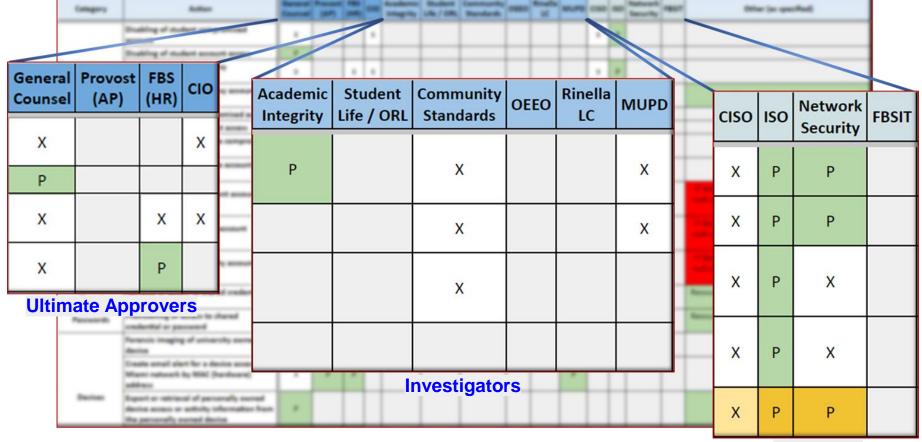
Why an ISAM

- Who has authority to approve an action?
- Can you remember who to ask every time?
- There are so many actions to keep track of
- Urgency can be a factor
- Keep up with changes and new requests



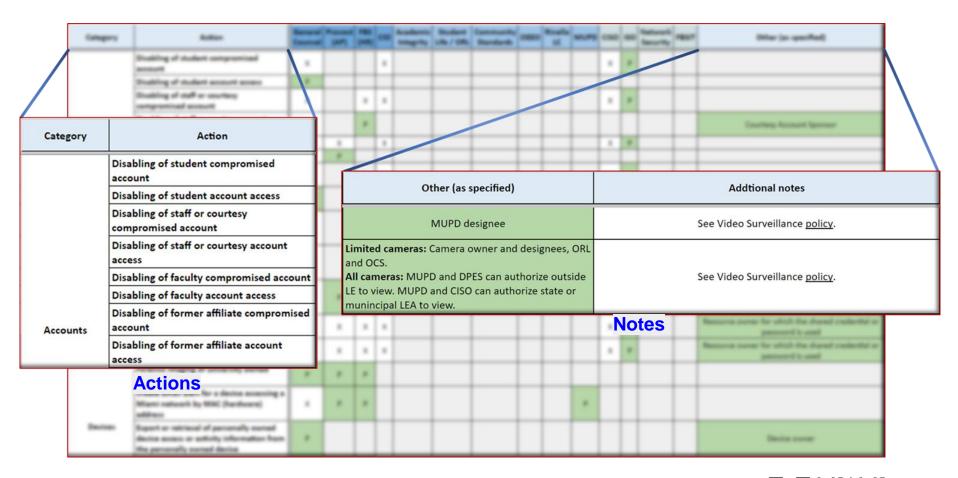
Category	Action	General Counsel	Provost (AP)	FBS (HR)		Academic Integrity	Student Life / ORL	Community Standards	OEEO	Rinella LC	MUPD	ciso	ISO	Network Security	FBSIT	Other (as specified)
	Disabling of student compromised account	X			X							x	Р			
	Disabling of student account access	Р														
	Disabling of staff or courtesy compromised account	X		X	X							Х	Р			
	Disabling of staff or courtesy account access	x		Р												Courtesy Account Sponsor
	Disabling of faculty compromised account	X	X		X							Х	Р			
	Disabling of faculty account access	X	Р													
Accounts	Disabling of former affiliate compromised account	x			x							X	Р			
	Disabling of former affiliate account access	Р														
	Export or retrieval of student account information or activity	х			x	Р					х	x	Р			IT Services' administrators are authorized to take such actions during the course of troubleshooting service issues.
	Export or retrieval of staff account information or activity	x		Р	x						х	x	Р			IT Services' administrators are authorized to take such actions during the course of troubleshooting service issues.
	Export or retrieval of faculty account information or activity	x	Р		x						х	X	Р			IT Services' administrators are authorized to take such actions during the course of troubleshooting service issues.
Shared Credentials and	Removal of access to shared credential or password	X	х	x	х							х	Р			Resource owner for which the shared credential or password is used
Passwords	Provisioning of access to shared credential or password	X	X	X	X							Х	Р			Resource owner for which the shared credential or password is used
	Forensic imaging of university owned device	Р	Р	Р												
	Create email alert for a device accessing a Miami network by MAC (hardware) address	х	Р	Р							Р					
Devices	Export or retrieval of personally owned device access or activity information from the personally owned device	Р														Device owner





Resolvers







Category	Action
	Disabling of student compromised account
	Disabling of student account access
	Disabling of staff or courtesy compromised account
	Disabling of staff or courtesy account access
	Disabling of faculty compromised account
	Disabling of faculty account access
Accounts	Disabling of former affiliate compromised account
	Disabling of former affiliate account access
	Export or retrieval of student account information or activity
	Export or retrieval of staff account information or activity
	Export or retrieval of faculty account information or activity
Shared Credentials and	Removal of access to shared credential or password
Passwords	Provisioning of access to shared credential or password
	Forensic imaging of university owned device
	Create email alert for a device accessing a Miami network by MAC (hardware) address
Devices	Export or retrieval of personally owned device access or activity information from the personally owned device
	Export or retrieval of university owned device access or activity information from a university owned device

Category	Action							
	Inbound block of non-Miami IP detected as a threat							
	Outbound block of non-Miami IP detecte as a threat							
	Outbound block of non-Miami URL detected as a threat							
	Inbound network block based on traffic signature							
Network	Outbound network block based on traffic signature							
	Export or retrieval of faculty or staff network location, authentication or activity information							
	Export or retrieval of student network location, authentication or activity information							
	Block of device by MAC address from network access							
	Transfer of faculty or staff Google Drive ownership to other specified staff member							
	Change of permissions to Google Drive file or folder or windows fileshare (elevating from view to editor, etc)							
	Removal of Google Drive or windows fileshare file access							
Files	Export or retrieval of faculty or staff owned Google Drive or windows fileshare file(s)							
	Export or retrieval of student owned Google Drive or windows fileshare file(s)							
	Export or retrieval of Google drive or windows fileshare file access history or activity							
	Export or retrieval of files stored on a university owned device							

	Removal of staff authorization or access to an application or system or service								
	Removal of faculty authorization or access to an application or system or service								
	Export or retrieval of student app or								
Applications,	system or service access or activity information								
Systems and Services	Export or retrieval of staff app or system or service access or activity information								
	Export or retrieval of faculty app or								
	system or service access or activity information								
	Removal of privileged access to an								
	application or system or service								
	Provisioning of privileged access to an								
	application or system or service to a specified person								
	Inbound block of non-Miami email								
	address sending spam								
	Inbound block of non-Miami email								
	address or domain sending phishing								
	Inbound block of non-Miami email								
	address sending abuse or harassment								
	Inbound quarantine or drop email filter								
	based on keyword or phrase								
	Viewing of faculty or staff email messa header information								
	Viewing of student email message header								
	information								
	Viewing of faculty or staff email message body								
Email	Viewing of student email message body								
	Faculty or staff email message retrieval or export								
	Student email message retrieval or export								
	Delegation of faculty or staff email access								
	to another MU account								
	Forwarding of faculty or staff email								
	Removal of email from faculty or staff mailbox								
	Removal of email from student mailbox								
	Removal of significantly malicious email from faculty, staff or student mailbox								

Action

Category

Category	Action									
Calendar	Export or retrieval of faculty or staff calendars information									
Calendar	Export or retrieval of student calendar information									
	Removal of website content									
Web Content	Hiding of Faculty or Employee information in the public directory									
	Export or retrieval of security camera footage									
Security Cameras	Playback or viewing of live or historical security camera footage									
	Removal of authorization or access to view camera footage									
	Provisioning of authorization or access to view camera footage (live or historical)									
Dhaaaaad	Export or retrieval of call center recording									
Phones and Voicemail	Export or retrieval of faculty or staff voicemail									
	Removal of access to swipe or tap doors									
Doors	Provisioning of access to swipe or tap doors									
	Export or retrieval of door swipe information									
Academic	Export or retrieval of student education records (FERPA)									
Academic	Export or retrieval of research data or records									





	Legend						
Р	Primary authorized approver						
X	Authorized to approve action						
	Not authorized to approve action						
Р	May be Primary authorized approver under some circumstances						
×	May be authorized to approve action under some circumstances						
Notes	Indicates recent policy change awaiting review by ISO						
Р	Indicates recent policy change awaiting approval by General Counsel office						
Position name	Ultimate approvers, if needed						
Office name Investigative offices							
Resolver office	Fulfillment offices						



A basic example

Demonstrates an email account delegation

Category	Action	General Counsel		FBS (HR)	Academic Integrity	Student Life / ORL	Community Standards	OFFO	Rinella LC	MUPD	ciso	ISO	Network Security	FBSIT	Addtional notes
Email	Delegation of faculty or staff email access to another MU account	x	Р	Р											An entity account's trustees are authorized to approve such delegation for the entity account.



A more complicated example

Shows variety across population types

Category	Action	General Counsel	Provost (AP)	FBS (HR)	сю	Academic Integrity	Student Life / ORL	Community Standards	OEEO	Rinella LC	MUPD	ciso	ISO	Network Security	FBSIT	Addtional notes
	Export or retrieval of student app or system or service access or activity information	x	Р		x	Р		x			x	x	Р			This would include a user's activity within an
Systems and	Export or retrieval of staff app or system or service access or activity information	x		Р	х			x			х	x	Р			application, system, or service such as page views within Canvas as well as associated timeframes and
Services	Export or retrieval of faculty app or system or service access or activity information	х	Р		x			x				x	Р			IP addresses in use.



Some additional scenarios

- Relative of deceased employee needs access to personal files or email
- **❖** Faculty requests student activity and location information
- Physical facilities wants security camera footage and door swipe records



What if ALL the approvers are out?

We follow a solid risk assessment practice

We are authorized to take deliberate and immediate action to protect the University



Upkeep is important

- **❖** There are occasional changes (OEEO, etc.)
- General Counsel approves every edit
- Awareness and training with other IT teams
- University distributed IT offices
- General population awareness



Audience participation

- **❖** What have you experienced?
- Can you share a story?
- What are your challenges?





Do they fit in the ISAM?

"Beat the ISAM - Improve the ISAM!"



What can you do tomorrow?

- Inventory your own approval requirements {categories, actions}
- Determine your own approval chains {approvers, investigators, resolvers}
- ❖ Reuse the MU [ISAM], or create your own



Questions?



Thank You

Get your own copy of the MU ISAM here.

NOTE: This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the <u>Creative Commons Attribution 4.0 International (CC BY 4.0)</u>, which grants usage to the general public, with appropriate credit to the author.

