Entity Name	Component/Group Name	Asset Name(s)	Threat Source	Threat Event	Vulnerability	Control	Control Response	Risk Likelihood	Risk Impact	Risk Rating	Risk Threshold	Global Notes	Component/ Control Notes	Risk Notes
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Insufficient Personnel Training	Security/Privacy Awareness and Training	In progress	4	5	20	8			2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Likely because not all staff have received update training on identifying different social engineering tactics or forms of safe data handling. I selected the Risk Impact of Severe because a successful social engineering attack could lead to all sorts of unauthorized disclosure of PII and legal penalties. 2025-04-19, Ethan Byrd, RR: I chose Mitigated as the recommended risk treatment strategy because the organization will be implementing strong controls to reduce the likelihood of a social engineering attack by making mandatory classes and response procedures. I reduced the residual risk from 20 to 5 because the implemented controls will greatly reduce the chance of an attack and lessen the potential damage through detection, knowledge and prepared staff.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Insufficient Personnel Training	Social Engineering Testing	In progress	4	5	20	8			2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Likely because not all staff have received update training on identifying different social engineering tactics or forms of safe data handling. I selected the Risk Impact of Severe because a successful social engineering attack could lead to all sorts of unauthorized disclosure of PII and legal penalties. 2025-04-19, Ethan Byrd, RR: I chose Mitigated as the recommended risk treatment strategy because the organization will be implementing strong controls to reduce the likelihood of a social engineering attack by making mandatory classes and response procedures. I reduced the residual risk from 20 to 5 because the implemented controls will greatly reduce the chance of an attack and lessen the potential damage through detection, knowledge and prepared staff.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Lack of Non-Disclosure Agreements	Non-Disclosure Agreements	No	4	5	20	8			2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Likely because there are currently no formal NDAs in place for staff and without them, there is a high chance that information could be disclosed. I selected the Risk Impact of Severe because the unauthorized disclosure of protected information or PII could result in FERPA or HIPAA violations. 2025-04-19, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because implementing Non-Disclosure Agreements will directly affect the risk of unauthorized disclosure of sensitive PII data and will help establish accountability. I reduced the residual risk from 20 to 5 because the addition and implementation of NDAs will greatly decrease the likelihood of undisclosed or malicious disclosure to very rare. While the impact remains severe due to what kind of data we are dealing with.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Insufficient Personnel Screening	Personnel Screening	In progress	3	5	15	8			2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Moderate because while not fully in place, there is still a chance of vetting someone with malicious intent or undisclosed risks. I selected the Risk Impact of Severe because if an unvetted gains access to student sensitive data, it could result in data breaches and reputational damage. 2025-04-19, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because implementing comprehensive personnel screening by including background checks, reference verification, helps ensure that individuals with access to sensitive systems and data are trustworthy and meet security standards. I reduced the residual risk from 15 to 4 because the addition of a formal personnel screening process lowers the Likelihood of a security or privacy incident from unscreened individuals to Rare. Although the Impact remains Major, the control significantly reduces the overall exposure by preventing unauthorized or high-risk individuals from gaining access in the first place.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Policy and Procedure Communication Deficiencies	Acceptable Use Policy	No	3	5	15	8			2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Moderatre because these policies are currently in progress of being put into place and staff are slowly learning however the potential misunderstanding can occur. I selected the Risk Impact of Severe because failure to enforce these policies and for them to be followed could allow for unwanted data access. 2025-04-20, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because making sure to add and improve upon the academy's policy framework will directly ensure compliance and practices and reduce the risk of security and privacy violations during data transfer and sharing. I reduced the residual risk from 15 to 5 because this addition will decrease the likelihood of policy related incidents to rare as clearer guidance and communication about systems and upgrades will help prevent data mishandling. However, it is still a major impact, as it can still lead to security breaches and legal consequences.

C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Policy and Procedure Communication Deficiencies	Information Disclosure Procedures	In progress	3	5	15	8	2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Moderatre because these policies are currently in progress of being put into place and staff are slowly learning however the potential misunderstanding can occur. I selected the Risk Impact of Severe because failure to enforce these policies and for them to be followed could allow for unwanted data access. 2025-04-20, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because making sure to add and improve upon the academy's policy framework will directly ensure compliance and practices and reduce the risk of security and privacy violations during data transfer and sharing. I reduced the residual risk from 15 to 5 because this addition will decrease the likelihood of policy related incidents to rare as clearer guidance and communication about systems and upgrades will help prevent data mishandling. However, it is still a major impact, as it can still lead to security breaches and legal consequences.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Policy and Procedure Communication Deficiencies	Information Systems Security Policies and Procedures	In progress	3	5	15	8	2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Moderatre because these policies are currently in progress of being put into place and staff are slowly learning however the potential misunderstanding can occur. I selected the Risk Impact of Severe because failure to enforce these policies and for them to be followed could allow for unwanted data access. 2025-04-20, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because making sure to add and improve upon the academy's policy framework will directly ensure compliance and practices and reduce the risk of security and privacy violations during data transfer and sharing. I reduced the residual risk from 15 to 5 because this addition will decrease the likelihood of policy related incidents to rare as clearer guidance and communication about systems and upgrades will help prevent data mishandling. However, it is still a major impact, as it can still lead to security breaches and legal consequences.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Policy and Procedure Communication Deficiencies	Policy and Procedure Communication	In progress	3	5	15	8	2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Moderatre because these policies are currently in progress of being put into place and staff are slowly learning however the potential misunderstanding can occur. I selected the Risk Impact of Severe because failure to enforce these policies and for them to be followed could allow for unwanted data access. 2025-04-20, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because making sure to add and improve upon the academy's policy framework will directly ensure compliance and practices and reduce the risk of security and privacy violations during data transfer and sharing. I reduced the residual risk from 15 to 5 because this addition will decrease the likelihood of policy related incidents to rare as clearer guidance and communication about systems and upgrades will help prevent data mishandling. However, it is still a major impact, as it can still lead to security breaches and legal consequences.
C7_Byrd_Et	Internal User / Internal User Group	CCS-DB, CMS-DB, IT-DB, Office-DB, PG-DB, SR-DB	Internal Parties	Improper Disclosure or Use of Sensitive Data	Lack of Policies and Procedures Enforcement	Personnel Sanctions	No	3	4	12	8	2025-04-19, Ethan Byrd, RD: I selected the Risk Likelihood of Moderate because there is a chance that without punishment for mishandling data or creating security risks, they may not learn their lesson and it could happen again with no formal way to handle it. I selected the Risk Impact of Major because the lack of clearly define sanctions increases the risk of policy violations and fosters a lack of accountability. 2025-04-19, Ethan Byrd, RR: I chose Mitigate as the recommended risk treatment strategy because with the addition of Personnel sanctions, there will be clear consequences for violations of security and privacy. I reduced the residual risk from 12 to 5 because implementing these controls will decrease the likelihood of an internal user violating policy violations set by the organization as they will be aware of the harsh consequences. The impact is still Severe as a policy violation can still lead to a FERPA and HIPPA violation.