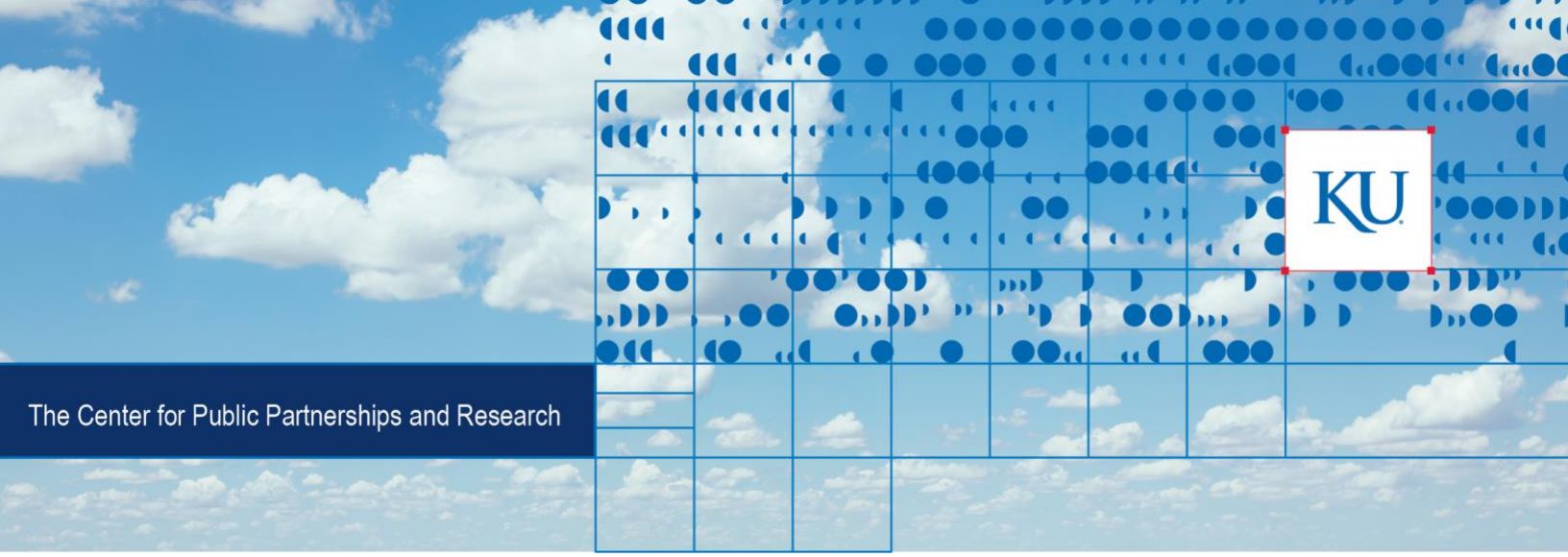

CPPR: Cybersecurity Audit

June 2025

Executive Summary

The *Center for Public Partnerships and Research* (CPPR) is a research, innovation and data-focused center within the University of Kansas' *Achievement & Assessment Institute* (AAI). As part of KU, CPPR operates under the governance and oversight of the University, and the State of Kansas Board of Regents (KBOR). CPPR supports state agencies, community organizations, and KU partners by managing several major data and technology platforms, including DAISEY, ROM and IRIS. Because of the sensitive data and critical servers we support, CPPR participates in regular cybersecurity assessments. This report summarizes the results of our 2025 assessment and outlines the steps we will take to further strengthen our security posture.

CPPR underwent a Cyber Security Assessment performed by RubinBrown, LLP (RubinBrown) between March 10th and June 2nd, 2025. This assessment utilized the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Special Publication (SP) 800-171 to measure our security posture.

CPPR is required to conduct Cyber Security Assessments on an annual basis. Results for each assessment will be posted.

Overall Performance

CPPR's cybersecurity posture demonstrates strong implementation of foundational controls and a clear commitment to continuous improvement. The recent assessment shows that **79% of shared and local controls are fully implemented**, with robust practices in areas such as identity and access management, encryption of data at rest and in transit, secure configuration management, and endpoint protection. CPPR also excels in maintaining hardware and software inventories, enforcing least privilege, and conducting regular vulnerability scans and penetration tests. These strengths reflect a mature approach to safeguarding sensitive data and critical systems.

Conclusion

CPPR is pleased to report moderate compliance in the majority of controls per this audit. Of the findings noted as needing improvement, we plan to address the following over the next 12 months.

- **Formalized Change Management** – We will implement documented approval workflows and standardized processes to ensure consistency across all environments.
- **Expanded Multi-Factor Authentication (MFA)** – We will review all SaaS platforms for MFA capability and apply compensating controls or risk exceptions where needed.
- **Continuous Monitoring & Governance** – We will establish a dashboard for real-time visibility into path compliance, open findings, and vendor status, reviewed monthly by leadership.

By addressing these areas, CPPR will advance from a managed state toward a defined and optimized cybersecurity program aligned with NIST 800-171 and CFS requirements.

For additional information regarding this report, please contact *CPPR@ku.edu*.

The Details: Findings by Category

Govern

CPPR maintains strong governance practices through clear communication channels with KU partners, vendors, and third parties, and by enforcing least-privilege access across all secure environments. All staff complete annual cybersecurity awareness trainings, with additional HIPAA, FERPA, and Human Subjects research training for compliance. CPPR IT manages and inventories all workstations, ensuring timely updates and end-of-life tracking. These measures reflect our commitment to security and operational integrity.

Moving forward, we will enhance governance by:

- formalizing a Risk Management Program for IRIS, ROM, and DAISEY.
- completing a Business Impact Analysis, and.
- documenting cybersecurity roles and responsibilities;
- implement a continuous-monitoring dashboard and establish quarterly governance reviews to align with NIST best practices.

Identify

CPPR operates under the least privileged access model. Unique accounts created for every user on all of our platforms. Physical end user machines placed into service and inventoried. Our hardware is monitored for end-of-life guidelines from our vendors. We monitor all of our systems including servers and regular endpoints for operating system versioning to ensure a timely transition at the end of life. The university conducts regular scans on all managed devices and regular scans of their network. We receive threat intelligence from the Cybersecurity & Infrastructure Security Agency (CISA).

Protect

CPPR and KU IT maintain strong safeguards to protect University technology assets and data. We have fully implemented configuration management practices, baseline configurations, least functionality settings, and secure software development standards. Endpoints and servers are managed through group policies, encryption, and regular patching, while hardware and software lifecycles are tracked to ensure timely replacement and secure disposal. Media sanitization is enforced using BIOS-level wipes or JAMF, followed by certified third-party shredding. These measures demonstrate our strength in maintaining secure configurations, managing hardware and software risks, and enforcing strict media protection policies.

Moving forward, we will enhance our posture by:

- formalizing change management approvals;
- improving documentation of access reviews, and;
- expanding MFA coverage for SaaS platforms;
- strengthen password management practices and implement continuous monitoring dashboards to ensure ongoing compliance and resilience.

Detect

CPPR and KU IT work together to ensure timely detection of potential cybersecurity threats and anomalies. KU IT provides continuous monitoring of networks, systems, and external service providers using enterprise tools like Rapid7 and Microsoft Defender, while CPPR supplements these efforts by reviewing SFTP logs, SQL logs, and other application-level indicators. We maintain processes for

correlating information from multiple sources and investigating adverse events in collaboration with KU IT. These practices demonstrate our strength in leveraging centralized monitoring and local log reviews to identify risks.

Moving forward, CPPR will enhance detection capabilities by:

- formalizing log review procedures;
- improving documentation of incident analysis, and;
- implementing a continuous-monitoring dashboard with key performance indicators (KPIs) for patch compliance and open findings.

These improvements will strengthen our ability to proactively identify and respond to potential threats.

Recover

CPPR relies on KU IT's enterprise-level incident response and recovery process to ensure continuity of operations after a cybersecurity event. Restoration capabilities for key applications are supported by KU IT and authorized vendors, with encrypted backups. CPPR is responsible for notifying users during the recovery phase and for confirming that all systems are restored meet operational requirements.

Moving forward, CPPR will enhance resilience by:

- formalizing recovery documentation for all managed environments;
- standardizing incident recovery workflows, and;
- implementing periodic tabletop exercises to validate restoration processes.

These improvements will ensure faster, more coordinated recovery and strengthen our ability to maintain critical services under adverse conditions.