CREC CENTER FOR REGIONAL ECONOMIC COMPETITIVENESS

DATA SECURITY CHECKLIST

The Data Security Checklist is based on the U.S. Department of Education's Privacy Technical Assistance Center (PTAC)'s *Data Governance Checklist* which is designed to summarize the key data privacy and security components required for successful data governance.

Data security and risk management

Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance plan.

Select from this list current organizational practices. Unchecked items are action items to develop successful data governance and be a data collaborator with federal agencies.

- ☐ Has a comprehensive security framework been developed, including administrative, physical, and technical procedures for addressing data security issues (such as data access and sharing restrictions, strong password management, regular staff screening and training, etc.)?
- ☐ Has a risk assessment been undertaken, including an evaluation of risks and vulnerabilities related to both intentional misuse of data by malicious individuals (e.g., hackers) and inadvertent disclosure by authorized users?
- ☐ Is a plan in place to mitigate the risks associated with intentional and inadvertent data breaches?
- ☐ Does the organization regularly monitor or audit data security?
- ☐ Have policies and procedures been established to ensure the continuity of data services in an event of a data breach, loss, or other disaster (this includes a disaster recovery plan)?
- ☐ Are policies in place to guide decisions about data exchanges and reporting, including sharing data (either in the form of individual records containing PII or as de-identified aggregate reports) with educational institutions, researchers, policymakers, parents, and third-party contractors?
- ☐ When sharing data, are appropriate procedures, such as sharing agreements, put in place to ensure that any PII remains strictly confidential and protected from unauthorized disclosure? Make certain that any data sharing agreements are allowed under local, state, and federal privacy laws and regulations, such as FERPA.
- ☐ Are appropriate procedures, such as rounding and cell suppression, being implemented to ensure that PII is not inadvertently disclosed in public aggregate reports and that the organization's data reporting practices remain in compliance with applicable local, state, and federal privacy laws and regulations (e.g., FERPA)?
- ☐ Are stakeholders, including eligible students or students' parents, regularly notified about their rights under applicable federal and state laws governing data privacy?

"Checklist: Data Governance." 2015. Protecting Student Privacy. U.S. Department of Education. June 2015. https://studentprivacy.ed.gov/resources/checklist-data-governance.