Organization Assurances for the LINK portal

(Needs to be signed by top official or designee of every educational organization (school corporations, networks, cooperatives, etc., referred to simply as organizations) which is permitting the cloud identities (Google, Microsoft, etc.) managed by their organization to use those identities to login to IDOE systems through the LINK portal.)

☐ By checking this box as an official representative of an educational organization in the state of Indiana, I [First Name] [Last Name] [e-mail] am consenting to permit the cloud identities established by my organization to serve as the usernames and passwords for accessing IDOE systems through the LINK portal. Additionally, I understand the expectations of my organization as outlined in the Organization Assurances below and my organization will abide by these expectations.

Organization Assurances

Use of Cloud Identities

A. We agree to register with the Indiana Department of Education the Internet domain associated with our organization.
B. We consent to allow our employees or designees for whom we have provided cloud identities (e.g., Google's G-Suite for Education, Microsoft's Office 365, or other approved cloud identity provider) to use these identities to access IDOE systems through the LINK portal.
C. We understand that any changes made to the domain by our organization may result in our employees and designees being unable to access IDOE systems through the LINK portal and that any such changes should be communicated to the IDOE prior to taking effect so that access to IDOE functionality is not interrupted.
D. We understand the responsibility for following best practices regarding identity management lies with our organization. We understand this responsibility extends to policies and protocols regarding password complexity, scheduled password resets, user training and cybersecurity awareness, and all other standard practices for ensuring account security.

Assignment of Roles and Responsibilities for Maintaining Appropriate Access to the LINK portal

E. We agree to name at least two Data Security Coordinators from our organization who will have the responsibility for assigning roles in the IDOE LINK portal.

F. We understand that access to IDOE systems will be assigned locally by our organizations' Data Security Coordinator and that these assignments should be done according to the principles and guidance of the Family Educational Rights and Privacy Act (FERPA) and any other applicable laws governing access to data. Users should be assigned roles giving data access appropriate to their position as a 'school official' within the organization and this access should be aligned to a 'legitimate educational interest' and "need to know." For example we understand that the access given to a teacher would be different than that given to a contractor or volunteer. Furthermore, we understand that we will use the guidance provided within FERPA regarding the definitions of 'school official' and 'legitimate educational interest' to determine what role each person using this system will have in order to assign the level of access to student data.
G. We understand it is the responsibility of the organization to determine the remedy to any issues stemming from inappropriate assignment of roles.

Local Policies and Practices for Identity Management

H. We agree to have a written policy in place indicating the local protocol for deprovisioning cloud identities for employees or designees of our organization when they leave employment or reach the end of contractual relationships with our organization. It is the expectation that this policy will provide for the timely termination of access to local systems and the deprovisioning of their cloud credentials. The deprovisioning of cloud identities at the local level will automatically remove access to the LINK portal based on those identities.
I. We understand the expectation that cloud identities provided by our organization are assigned to a single employee or designee of our organization and that these credentials are not shared across individuals in any way.
J. We understand that misuse of cloud identities by our employees or designees leading to inappropriate access to data in the IDOE LINK portal may result in termination of access and additional investigation and corrective action by the IDOE.

IDOE Audits and Responsibilities

K. We understand the IDOE reserves the right to conduct audits of all access provided to the system (the LINK portal) as well as actual logins and time spent on the system.
L. We understand the IDOE is responsible for providing access to IDOE systems for educators and for maintaining lists of roles for each user indicated by Data Security Coordinators within each educational organization.