Lake Geauga Computer Association

Software Support SLA

Statement of Intent

The Information Technology Center LGCA and school district mutually agree that this Service Level Agreement (SLA) documents all software support services provided by the ITC that are required by a school district. This document defines the schedule of services, performance deliverables, and the methods by which services are delivered. Both parties share responsibilities under this agreement as described below.

Category Definition

This Service Level Agreement addresses the following software support categories:

ITC

1. Software management
2. Data management
3. Training
4. Problem resolution
5. Documentation
6. Communication
7. Quality of service

District

1. Software management
2. Data management
3. Training
4. Problem resolution
5. Documentation
6. Communication
7. Quality of Service

ITC

1. Hours of Operation
2. System Availability
3. Security Policy
4. Password Policy

Assumptions/Responsibilities

The district and the ITC must have a reciprocal relationship in order to facilitate high quality delivery of service. Listed below are the responsibilities of both.

ITC

1. Software management.
    a. Install new versions and patches according to specified timeframes.
    b. Maintain appropriate application environment (hardware, operating system).
    c. Create and maintain cost-effective software license and annual maintenance agreements.
    d. Maintain compliance with industry standards to facilitate interoperability of software applications.
    e. Develop routines to enable interoperability between software applications.
    f. Explore new software applications for the benefit of the district.
2. Data management
    a. Generate backups on a nightly basis.
    b. Maintain and manage offsite storage according to the site's business continuity/disaster recovery plan.
    c. Data retrieval will occur in conjunction with district personnel based upon timeframes established in the Operating Guidelines (i.e., these will be application-specific).
    d. Restore data critical for daily district operations as a top priority according to the site's backup and recovery procedures as defined in the disaster recovery document.
    e. Enable data transfer between systems.
3. User training
    a. Provide all user training in a timely and adequate fashion, as defined by the support staff and operating committees.
    b. Track user attendance and assess user training needs.
    c. New user training will be offered at least once per year.
4. Problem resolution
    a. Maintain a qualified staff commensurate with staff budget.
        i. Professional "code of conduct" is customer-centric.
        ii. Facilitate continuing education for all staff per rules defined in Ohio Administrative Code.
    b. Maintain software support contracts with third parties.
    c. Provide helpdesk support as defined in timeframe/availability.
    d. Assess frequency and nature of questions from the district and use this information to plan for future training.
    e. Log problems using HelpDesk software when available.
5. Documentation
    a. Provide documentation based upon user needs.
        i. Types of documentation can include user guides, release notes, frequently asked questions, checklists, Forums, and knowledge base.
        ii. Content can include best practices, supplements to ODE or vendor documentation (i.e., EMIS Guide), and step-by-step software use guidance.
    b. Enable access to documentation via hard copy and the web.
    c. Organize documentation in a manner that facilitates user access and usability.
    d. Update documentation based on anticipated user demand for changes.

6. Communication
    a. Notify district of application-driven hardware (e.g., desktop or printer) specifications.
    b. Notify district of release of new versions or patches after appropriate pre-release site testing.
    c. Communicate based upon user needs.
        i. Methods can include email messages, newsletters, site visits, telephone calls, meetings (e.g., user groups, governing board, advisory committees), and web site updates.
        ii. Chosen method will be based upon nature and urgency of topic.
        iii. More than one method may be used based on priority level.
    d. Keep up to date on all district software communications.
7. Quality of service.
    a. Measure customer satisfaction through an annual survey AND assess incremental progress through at least one other recommended method (e.g., post-training evaluations, caller logs, service desk surveys generated after problem resolution).
    b. Assessment results from annual audit (i.e., SAS-70 report) for process improvements.
    c. Self-evaluate performance and progress within the context of the annual continuous improvement plan provided to the Ohio Department of Education.

School District

1. Software management
    a. Implement new features associated with updated versions of software if the new features are found to be beneficial to the district.
    b. Ensure that user's workstation hardware meets the minimum application specifications and the software environment is appropriately configured for software usage.
    c. Ensure that appropriate licenses are issued and maintained for all users.
    d. Ensure that appropriate authorizations (including signoff from all parties) are in place for access to software.
    e. Define new software requirements for new or existing applications to the ITC using recommended mechanisms as feasible or informally as needed.
    f. Participate in opportunities (e.g, surveys, demonstrations, user group meetings) facilitated by the ITC to explore new or innovative usage of software applications.
    g. Work with ITC to mutually define additional resources (both financial and personnel) required for successful implementation of new software.
2. Data management
    a. Upon detection, immediately notify the appropriate ITC contact person as to specific data retrieval needs.
    b. Be responsible for rebuilding any lost data after restoration.
    c. Meet all published timelines (including but not limited to those set by State Auditor, financial institutions, ODE, and the ITC) for submission of data.
    d. Maintain appropriate security policies for protection of data.
3. Training
    a. Newly assigned employees will attend appropriate district, vendor, and/or ITC training.
    b. Alert ITCs to ongoing training needs.
    c. Complete evaluation forms to provide immediate feedback and to improve future training sessions.
    d. District leadership will assign appropriate staff to ITC Operating Committees, attend training sessions and ensure appropriate software authorization. "Appropriate staff" is defined as staff with basic computer skills and expertise in the area associated with the software application.
4. Problem resolution
    a. Maintain and implement a set of procedures (e.g., communication and escalation) for internal software support.
    b. Follow the rules and procedures for reporting problems to the ITC as specified as follows:
        i. Reporting of initial problems will be handled through electronic means (preferred) or telephone.
        ii. Initial reporting of the problem will include as much detailed information or documentation (e.g., screen shots, reports, actions taken by user prior to problem occurrence, attempted solutions) as possible.
        iii. After initial problem report, user will be available for and respond to inquiry regarding problem reported.
        iv. If problem reported is solved by the district staff, staff will notify ITC as soon as possible.
        v. Reporting of initial problem to ITC will be made to ONE point of contact, not to multiple individuals, to reduce duplication of effort.
        vi. If problem is not resolved to the satisfaction of the district staff the following escalation procedure shall be followed;
            1. ITC application support staff shall be notified
            2. ITC Director shall be notified
            3. ITC Executive Director shall be notified
            4. ITC Board Chairperson shall be notified

5. Documentation
    a. Review all documentation and updates within the timeframes specified by the ITC.
    b. Use latest versions of documentation.
    c. Inform ITC regarding accuracy, usability, relevance, and availability of -- and future needs for -- documentation in a timely fashion.
6. Communication
    a. Notify ITC immediately of relevant staff changes.
    b. Keep up to date on all ITC software communications.
7. Quality of service.
    a. Measurement of customer satisfaction will be handled by an annual survey AND incrementally through at least one of the other recommended methods (e.g., post-training evaluations, caller logs, service desk surveys generated after problem resolution).
    b. Assessment of results from annual audit (i.e., SAS-70 report) for process improvements.
    c. Self-evaluation within the context of the annual CIP report provided to the Ohio Department of Education.
    d. Participate in any other quality of service review processes based on guidance from the Ohio Regional Education Delivery System and specific Regional Service Center requirements.
8. Quality of service
    a. Complete incremental and annual surveys administered by ITC.
    b. Provide feedback via focus groups, advisory groups, and other subcommittees to help gauge customer satisfaction and make recommendations for improvement.
    c. Participate in any other quality of service review processes based on guidance from the Ohio Regional Education Delivery System and specific Regional Service Center requirements.

Hours of Operation

LGCA will maintain the following hours of operation. Reasonable attempts will be made to have all departments covered during the hours of operation by staggering staff start/stop times.

School Year
Monday thru Friday
7:30 a.m. to 5:00 p.m.
Excluding Holidays

Observed Holidays
Martin Luther King Day
President's Day
Good Friday
Memorial Day
Independence Day
Labor Day
Thanksgiving Day
Day after Thanksgiving
Christmas Eve Day
Christmas Day
New Years Eve Day
New Years Day

When a holiday falls on Saturday, LGCA will be closed on Friday.
When a holiday falls on Sunday, LGCA will be closed on Monday.
Any changes users will be notified via email.

Calamity days
Calamity days – office will be covered, unless treacherous conditions users will be notified via email.

System Availability

LGCA will make every effort to maintain 100% availability of the software applications during normal business hours with the exception of maintenance issues as outlined below. The guidelines below will be utilized for maintenance exceptions.

Systems and Network Maintenance Guidelines

1. **Hardware or software failure, immediate, without warning**
    a. Alert users and staff if possible
    b. Begin work to restore service immediately
    c. Alert users and staff as to anticipated downtime
    d. If downtime is of severe nature and downtime is anticipated to be an extended period, LGCA staff will divide a list of districts and call each board of education.
    e. Alert users and staff when services restored

2. **Hardware or software failure, imminent** (This could be a failing disk drive, software application, or network issue)
    a. Review urgency of problem with management or other staff
    b. Determine time to disable service
    c. Alert users and staff regarding issue, timelines
    d. Begin work as scheduled
    e. Alert users and staff when services restored

3. **Hardware or software upgrade, 3rd party technical support required and only available during business hours**
    a. Review urgency of problem with management or other staff
    b. Determine availability of 3rd party technical support
    c. Determine time to disable service, preferably in the late afternoon
    d. Alert users and staff regarding issue, timelines. When possible, give users 24 hour or more notice.
    e. Begin work as scheduled
    f. Alert users and staff when services restored

4. **Hardware or software upgrade, 3rd party technical support available 24/7 or not needed**
    a. Review urgency of problem with management or other staff
    b. If needed, determine availability of 3rd party technical support
    c. Determine time to disable service, preferably after 4:30, late evening or weekend hours.
    d. Alert users and staff regarding issue, timelines. When possible, give users 24 hour or more notice.
    e. Begin work as scheduled
    f. Alert users and staff when services restored

Email notification shall include the following
Describe issue and it's impact on users
Define user community impacted-see below for list
Define timelines, when is service going down, when will service be restored
Send follow-up email after service is restored

Email Lists by Application / Service

All Services: Special List Created for a single announcement to reduce SPAM
Internet Services: **lgca_tech@lgca.org**
Fiscal Services: **mail_treas@LGCA.org**, **local_acct@lgca.org** , **local_payroll@lgca.org**
Media Services: **infohio@lgca.org** **infohio_librarians@lgca.org**
Infinite Campus Services: **district_contact@lgca.org**

LAKE GEAUGA COMPUTER ASSOCIATION

DATA SECURITY POLICY AND PROCEDURES

Data System Security Policy

The General Assembly and staff of Lake Geauga Computer Association (hereafter referred to as the Computer Center) recognizes that data maintained by the Computer Center is the legal property of the School District (hereafter referred to as the district) which entered such data or to which such data is assigned. Each district's individual portion of the Computer Center's computer which maintains district data is considered an extension of the district. The Computer Center, therefore, is a holder in public trust of the data.

The Assembly adopts the following policy statements concerning access to and security of the data. These statements are intended to assure the inviolability of the data, provide for procedures to permit authorized access to data and prohibit unauthorized release of data, and recommend features which districts and the computer Center can implement to promote system and data security.

I. Data Access

Data maintained by the Computer Center shall be recognized as the exclusive property of the district. Each district shall be in control of its own data maintained at the Computer Center. Access to the data shall be granted as follows

A. District Personnel

1. District personnel shall be granted access upon the written authorization of the District's Superintendent and Treasurer.

2. Such access may be restricted (as may be practical or technically possible) to certain data sets and/or specific access types.

3. The Computer Center shall provide a standard form for authorization.

B. Computer Center Personnel

1. Computer Center staff shall be granted access when such access is within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities.

C. Outside Access

1. Outside access shall be granted upon the written authorization from the superintendent of the district or his/her designee.

   a. "Outside" is defined as any individual or group of individuals not belonging to the School District or the Computer Center.

2. Data required to be transferred to the Ohio Department of Education shall be as defined by statute, State Board of Education Rule, and/or as outlined in the Education Management Information System Definitions, Procedures and Guidelines.

3. Written confirmation of the outside access shall be forwarded to the district superintendent within 24 hours.

II. Data Security Procedures

The first point of security is access to the computer system and its data via the local network of users. To enhance security and reduce the risk of unauthorized access, the following guidelines shall be followed:

A. Users will be assigned one unique account for access to the system.

B. Each user account shall require a password with a minimum of 6 characters. This password shall be treated as confidential information by the users. Users are responsible to safeguard their passwords, other access protocols, and district and Computer Center information, in whatever form. No list of passwords shall be maintained by the Computer Center or the District.

C. All users will be required by the system to change their password or at least every 90 days; "captive" accounts (accounts which have access to only limited, non-system programs and commands) must have their passwords assigned by the Computer Center and shall be changed at least every year.

D. A review of user account activity will be performed quarterly by the computer staff. User accounts that have not been accessed in the previous 180 days will be disabled; users not accessing their account in the previous 90 days will be notified that such inactivity may cause their account to be disabled. Users should ensure their terminals, when not in use, are properly logged off the system.

E. Users shall be granted only those privileges consistent with the duties and responsibilities of their position. Authorized privileges shall be grouped in a "normal" and "extended" category: "normal" privileges are granted by the system when a user logs onto the system and represent the privileges required to perform the users normal duties; "extended" privileges are those privileges which the user may be authorized to use, but which must be specifically enabled by user before being utilized.

F. Access to the computer system via an electronic network outside the Computer Center area will be restricted to the minimum level of access necessary for authorized users. No "general access" accounts shall be maintained.

G. Access to privileged or system accounts shall only occur with the authorization of the Computer Center Director. Following outside access to a privileged account, the account password shall be changed to prevent further access without the Computer Center staff's knowledge.

H. Audit Log
Sufficient audit alarms shall be enabled to track attempts to break into a user or system account and other security-related events. The audit log shall be reviewed daily for suspicious entries and shall be filed for future reference.

I. Notification by district users
1. For security reasons, each district should immediately notify the Computer Center if an employee has been terminated or has left the district. The accounts and files of the employees shall be disabled immediately and deleted within five business days.

2. Each district should notify the Computer Center when any district user is placed on leave of absence, or short-term or long-term disability. The user's account shall be completely disabled and re-opened only at the request of the user's immediate supervisor.

J. In all events, the Director of Computer Services shall have the authority and responsibility to take actions necessary to insure the integrity of the data and security of the computer system, or to enable authorized district users to utilize the computer system to fulfill the duties associated with their positions.

K. The data security policy and procedures shall reviewed annually.

L. Current District Personnel Authorization List Attached.