Department of Information Technology
Global Service Levels

Objective

This DIT Global Service Level Agreement describes the core IT Service components, (such as Incident record handling), documents pertinent Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer.

The Global Service Level Agreement includes:

- General and specific areas of support and targets applicable to every DIT service
- Levels of support and targets applicable to a specific service; including responsibilities of DIT and the customer.
- MOU: Optional customer specific requirements (additions or changes)
- If there are content differences, information documented in the Service SLA takes precedence over the information stated in the Global Service Levels. In addition, information contained in an MOU associated with a standard service also takes precedence over the information contained in the Service SLA and/or the Global Service Levels.

Global Service Levels

Service Support

The DIT Service Desk operates 24 x 7 x 365 and offers a single point of contact for all customer inquiries related to DIT services for the State of North Carolina's business and technical infrastructures. The DIT Service Desk agents provide business and technical infrastructure analysis, problem solving, and first and second level diagnostics.

Hours of Operation

DIT Services are available 24 x 7, excluding planned outage maintenance windows and unavoidable events. Maintenance windows are used only when needed for planned changes that have gone through the DIT Change Management Process. In addition to the Standard DIT Maintenance Windows, site-specific changes may be coordinated with customers at non-standard times.

DIT Standard maintenance windows include:

- 4:00 a.m. to 7:00 a.m. each Thursday
- 4:00 a.m. to 12:00 p.m. each Sunday

Any service maintenance windows outside of these standard windows are documented in the service specific SLA.

Contacting Support and Ticket Escalation

The DIT Service Desk is the single point of contact for initiating all Incidents and Service Requests, including any requests for ticket escalation. Customers may contact the DIT Service Desk at 919-754-6000 or toll free at 1-800-722-3946 or via email at dit.incidents@its.nc.gov.

The Business Relationship Manager assigned to your agency is available to address any questions regarding DIT services, processes or information technology business needs. You may contact your Business Relationship Manager directly or initiate a Service Request with the DIT Service Desk.

Incidents and Service Requests

Ticket Creation and Prioritization

Two types of tickets may be created by contacting the DIT Service Desk. An Incident is any disruption of service. A Service Request is a request for information or a request for a new service or to change an existing service. Customers may open an Incident or a Service Request ticket by calling or initiating an email to the DIT Service Desk.

It is important to note that tickets received via email are categorized as a low priority. Therefore, any critical or high Incident or Service Request should be **initiated by calling** the DIT Service Desk. If a critical or high Incident or Service Request is initiated by e-mail**, it must be followed up with a telephone call to the Service Desk** to ensure proper prioritization. Failure to call may result in a low priority ticket. When sending an email, summarize the nature of the Incident or Service Request in the Subject field.

Upon ticket creation, the customer will automatically be emailed a Receipt Confirmation with the ticket or reference number. This confirmation notes that the Incident or Service Request has been logged at the DIT Service Desk and that it is being assigned to a work group.
Customers are responsible for ensuring their email address is provided to the DIT Service Desk for update and resolution notification purposes.

The DIT Service Desk assigns a Priority to every initiated Incident or Service Request. The DIT Prioritization Model is used to ensure a consistent approach to define the sequence for a ticket to be handled and to drive the assignment of resources.

The Priority assigned to a ticket depends upon:

- The Impact on the business: size, scope and complexity of the Incident
- The Urgency to the business: time within which resolution is required

Incident Target Resolution Times

The Incident Target Resolution Time is the total time from ticket creation to Incident resolution (restoration of service to the user). Service may be restored either through a workaround or a permanent solution. DIT is committed to resolve ninety percent (90%) of Incidents within the time frame specified for each Priority.

The following chart shows the target resolution times by Priority after the initial assessment/assignment of an Incident by the Service Desk.

Incident Priority	Target Resolution Time
Critical	4 hours or less
High	8 hours or less
Medium	24 hours or less
Low	3 business days

Change Management

DIT has a Change Management Process with the goal of protecting the shared environment of the State's infrastructure from unintended impacts as a result of Changes made to the various systems, applications, and equipment operating on the enterprise network and in the State Data Centers managed by DIT.

Additionally, DIT sponsors the Enterprise Change Advisory Board (ECAB), whose membership consists of agency and DIT representatives. The ECAB meets regularly to communicate all Extensive, Wide-Spread and Significant/Large Changes that impact DIT and multiple Agencies.

All ECAB members must adhere to the following guidelines:

- Customers will have an Agency representative attend and participate in the ECAB
- Customers will notify DIT of any Agency planned Changes to the DIT provided infrastructure
- DIT will review any Agency Change that impacts the DIT managed infrastructure; if no impact is found, the Change will be approved.

Two levels or types of Changes are considered for ECAB (Extensive/Wide-Spread and Significant/Large). These are represented by the Lead Times and Impacts detailed below:

Impact		
Extensive/Widespread **30 calendar days**	**Definition**	**Major Business Impact:** A change to a Service or Application that will/could result in an outage with no workaround resulting in complete loss of Service or Application availability.
	Example	• A zero point release/upgrade • Core Hardware and Configuration affecting all state operations • Requires the coordination of multiple Service teams • Back out plans are extensive, time consuming, and expensive
Significant/Large **14 calendar days**	**Definition**	**Significant Business Impact:** A change to a Service or Application that will/could result in a significant loss or degraded of Service or Application availability.
	Example	• Any change that affects the Service Desk operations • Core Hardware and Configuration affecting two (2) or more agencies • May require the coordination of multiple Service teams • Vendor Service Pack • Back out plans are moderately difficult to execute and time consuming

Customer Communication

DIT will update customers as tickets are being worked, as well as when tickets are resolved. DIT will also provide communications, through the DIT Customer Communications Hub, when Incidents or outages occur that may impact the customer. Customers of DIT should visit the DIT Customer Communication Hub at https://communications.its.state.nc.us/ to self-register for communications regarding services and to view service status. Customers may also subscribe to the Projected Service Outage Report via the Communications Hub which provides information regarding upcoming change events that have the potential to impact services and lines of business.

If an Incident is causing major impact, or potentially major impact, to the business and requires a response that is above and beyond that given to standard incidents, a Major Incident Plan (MIP) may be declared. MIPs are prioritized as critical incidents and require cross-agency coordination, management escalation, the mobilization of additional resources, and increased communications. Depending upon the customer impact, DIT may provide communications to Agency contacts using various methods internally. The Business Relationship Managers work with their respective agencies to maintain updated MIP contact information.

Security Standards and Policies

DIT services adhere to DIT and State CIO Security Standards and Policies. The Customer is responsible for ensuring that their systems, applications, processes and data are compliant with and follow State CIO Security Standards and Policies. As an example, the Customer is responsible for classifying their data and identifying additional security that may be required for data classifications such as PII, HIPPA, PCI or IRS 1075.

Risk Management

DIT provides business continuity services, including assistance with continuity planning strategies, to help agencies comply with G.S. 147-33.89. Other services include the availability of dual sites for application hosting, testing, and disaster recovery. DIT conducts a minimum of two disaster recovery exercises each year for its critical applications; hosted agencies are invited to participate. The customer is responsible for determining their disaster recovery objectives and purchasing any additional services or equipment that may be required to meet those objectives.

Customer and DIT Access and Assets

Protection of equipment

Agencies/Customers must protect all DIT owned assets that are resident at agency locations or being used by agency personnel or contractors (NC State Security Policy Chapter two). While the agency/customer is responsible for the physical security of the assets, DIT is responsible to replace DIT owned assets that are lost, damaged or stolen while on agency premises and/or in use by agency employees or contractors.

Site Environmental Responsibility

Agencies/Customers must provide, protect, control and monitor any onsite environmental requirements associated with the presence of DIT owned assets (NC State Security Policy Chapter nine). This includes HVAC, Static electricity, humidity, air circulation, electrical circuits and line fluctuations, flooding, physical access, space management, and BCP/DR plans for the environmental controls.

- If a new location or site is being considered for DIT Services, a site survey will be conducted by DIT staff to determine if there are environmental concerns or other issues that need to be addressed as part of the service provisioning process. Any issues that cannot be addressed or that are non-standard will be documented in an MOU, including additional costs (if applicable) and other actions needed to mitigate the risk or concern.

Customer Access to Agency Owned Assets

The customer shall have access rights to their assets for the purpose of application monitoring and for managing software licenses and application code.

DIT Physical and Remote Access and changes to DIT equipment on customer premises

- Agencies and customers of DIT must provide timely physical site access to DIT Staff so that DIT can provide the necessary support for the services being provided to that location. Access must be provided to DIT assets located on agency premises, including access to server closets, wiring closets, switches and other DIT managed devices.
- DIT staff must adhere to an agency's security access requirements, i.e. signing a visitor's access log.
- DIT must ensure that the agency is notified when DIT staff no longer require badge access to the agency's facility.
    - When changes are made to DIT assets, DIT and its customers must adhere to the security standards associated with the asset (NC State Security Policy Chapter two), and follow the DIT Change Management Process.
    - Agencies and customers of DIT agree to permit DIT to open all required firewall ports necessary for DIT to provide services and management of DIT remote equipment in the Agency.

On-boarding and off-boarding of State employees and contractors.

Agencies need to submit a ticket to the DIT Service Desk for the on-boarding and off-boarding of agency employees/contractors when they are entitled to receive support for any DIT service. In addition, DIT owned assets deployed to agency employees/contractors must be returned to DIT for proper equipment cleanup and potential reuse.

Financial Authorization

Agencies must provide DIT with written assurances through the appropriate services provisioning process, that funds are available to cover the requisition of the new equipment or services being purchased from DIT, and that all invoices will be paid promptly and fully upon receipt, consistent with State accounts payable practices. Agencies should open a ticket with the DIT Service Desk if there are any questions or disputes with the DIT bill.

Service Level Reviews

DIT shall conduct regular meetings with executive branch agencies (customer) to review service level achievements, service support and Service Level Agreements (SLAs). These Service Reviews will be facilitated by the DIT Support Services group and will be conducted at a minimum on an annual basis or as agreed upon by the customer. A Business Relationship Manager and the customer will participate in the reviews.

A customer's SLA Report will be discussed. The SLA Report displays service level achievements, such as metrics and details for Incidents and Service Requests. Applicable SLAs will also be reviewed with the customer whenever there is a significant change to the delivery of the service.

Dispute Resolution

The Parties (DIT and the Customer) agree that it is in their mutual best interest to resolve disputes informally and amicably. If representatives of the Parties are unable to resolve any dispute after reasonable negotiation, such issue shall be escalated to the respective legal counsel of the Parties, and then, if necessary, to the heads of the respective agencies. If the dispute still remains unresolved, then either Party may seek resolution using the mechanism set out in N.C.G.S. 147-33.93 Fees; Dispute Resolution Panel.

Confidentiality

As a result of this SLA, each Party (DIT and the Customer) are likely to have access to information or records of the other Party that are exempt from disclosure under applicable law. Such information shall be deemed "Confidential Information." Each Party shall maintain all Confidential Information of the other Party in the strictest confidence and will not at any time use, publish, reproduce or disclose any Confidential Information, except to the extent necessary to carry out the Party's duties under this SLA or as expressly authorized in writing by the other Party.

Each Party shall, prior to disclosing any Confidential Information to any contractor or other third party, promptly seek and obtain authorization for the disclosure from the other Party and shall ensure that the contractor or other third party is subject to a non-disclosure agreement enforceable in North Carolina. Nothing in this paragraph is intended to prevent either Party from compliance with any order issued by a North Carolina state or federal court.

Ownership and Custody of Data

All data or other records held or stored by DIT as a result of this SLA shall be considered the property of, and in the custody of, the Customer. Customers should ensure their backup, retention and business continuity requirements for customer owned data are clearly identified in the SLA. In the event of a request made to DIT for access to Customer records pursuant to the North Carolina Public Records Act or by other legal process, DIT will decline such requests and indicate to the requestor, that DIT is not the custodian of such records. DIT will refer the requestor to the Customer and will notify the Customer of such request as soon as is reasonable under the circumstances, in order to provide the Customer with an opportunity to state or otherwise argue its own position concerning such request.