Development Consultants Incorporated (DCI)
Supplemental Customer Service Agreement

Table of Contents

Supplemental Customer Service Agreement 1
General 2
Information Transfer 2
Risk Management 2
Incident Management 3
Service Requirements 3
Service Changes 5
Service Removal 5
Service Delivery 5
Relationship Management 6
Control Processes 8
Change Management 8
Release Management 8

General

Development Consultants Incorporated (“DCI”, “Our”, “We”, or “Us”) is a provider of Information Technology professional and cloud services. This Development Consultants Incorporated Supplemental Customer Service Agreement (the "Agreement") is made and entered into by and between Development Consultants Incorporated and the entity agreeing to these terms ("Customer", “Consumer”, “You”, or “Your”). The Supplemental Agreement establishes a common understanding of the Quality Management, Service Management, and Information Security Management terminology, policies, and procedures in place by DCI. This agreement, together with any applicable agreements, contracts, schedules, purchase orders, service orders, appendices, or attachments, constitutes the terms of the relationship between DCI and the Customer.

Information Transfer

Prior to transmitting business information electronically or via physical media, the sender and receiver agree that:

- The sender and receiver shall agree, on a case-by-case basis, to the technical standards for recording and reading information and software;
- The sender shall determine any special controls that are required to protect sensitive items, cryptography shall be used for the transmission of all electronic data;
- The sender shall maintain a chain of custody for the information until it is received by the receiver;
- The sender shall determine acceptable levels of access control commensurate with the classification of the information;
- The sender is responsible for management of the control and notification of transmission, dispatch, and request for receipt;
- The sender shall determine the minimum technical standards for packaging and transmission;
- The sender shall determine if an escrow services are required and determine the escrow value, terms, and beneficiaries;
- The sender shall determine an appropriate courier capable of maintaining a chain of custody and sufficient insurance to cover the estimated value of the information, as required;
- The sender shall use procedures to ensure traceability and non-repudiation of the transmission, as required;
- The sender shall be responsible and liable in the event of any information security incidents while the information, such as leakage or loss of data. The receiver shall not accept or access classified information or material for which the receiver has not been granted access or does not have the proper clearance. The receiver shall report all security violations or suspected compromises to their information security manager and security@devconinc.com immediately; and
- The sender shall establish the use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected.

Risk Management

Risk is defined as the effect of uncertainty on objectives and could have either a positive or negative impact to one or more interested parties should that risk occur. International Standard ISO 27005

identifies four primary risk treatment options: risk modification, risk retention, risk avoidance, and risk sharing.

DCI and the Customer agree that the preferred risk treatment option is risk avoidance and agree to coordinate risk management activities to avoid risk wherever practicable. If an identified risk is unavoidable, or risk avoidance is impractical, both parties agree to coordinate risk treatment activities to modify, share, or retain the risk.

Incident Management

An incident is defined as unplanned interruption to a service, a reduction in the quality of a service, or an event that has not yet impacted the services to the Customer.

DCI and the Customer agree that a *major incident* is defined as an event which has significant impact or urgency for the business/organization and which demands a higher priority response than the routine incident management process.

A major incident will be an incident which:

- may either cause, or have the potential to cause, impact on business-critical services or systems;
- or be an incident that has significant impact on reputation, legal compliance, regulation or security of the business/organization

DCI and the Customer will agree upon the priority of an incident at receipt of the incident or service request, or as soon as possible afterwards. Throughout the DCI Incident Management Process, DCI in coordination with the Customer may reassess an incident's impact or urgency due to changing conditions or new information. DCI will resolve incidents in accordance with the Service Level Agreement that corresponds to the incident's classification.

Service Requirements

If not explicitly defined elsewhere, DCI and the Customer agree to the following Service Levels:

Issue Type	Definition	Target Time to First Response	Calendar
Major Incident	A major incident is defined as an event which has significant impact or urgency for the organization and which demands a response beyond the routine incident management process. A major incident will be an Incident which: may either cause, or have the potential to cause, impact on business-critical services or systems; or be an incident that has significant impact on reputation, legal compliance, regulation or security of the organization.	15m	24x7
Information Security Incident	An Information Security Incident is made up of one or more unwanted or unexpected information security events that	15m	24x7

Issue Type	Definition	Target Time to First Response	Calendar
	could possibly compromise the security of information and weaken or impair business operations.		
Incident	An Incident is an unplanned interruption to a service, a reduction in the quality of a service, or an event that has not yet impacted the services to the Customer.	2h	24x7
Access Request (Standard)	A Standard Access Request is a request to create or modify user-level access on a controlled information system.	8h	24x7
Access Request (Privileged)	An Administrative Access Request is a request to create or modify privileged access on a controlled information system.	8h	24x7
Change Request	A proposal for a change to be made to a service, service component, or management system.	8h	9-5
Service Request	A request for information, advice, access to a service or a pre-approved change.	16h	9-5
AWS Business-critical system down	Your business is at risk. Critical functions of your application are unavailable.*	15m	24x7
AWS Production System Down	Your business is significantly impacted. Important functions of your application are unavailable.**	1h	24x7
AWS Production System Impaired	Important functions of your application are impaired or degraded.**	4h	24x7
AWS System Impaired	Non-critical functions of your application are behaving abnormally, or you have a time-sensitive development question.**	12h	24x7
AWS General Guidance	You have a general development question, or you want to request a feature.**	24h	24x7
All remaining issues	Any low impact and low urgency issue that does not match any other issue type.	24h	9-5

* Available to DCI AWS Customers with Enterprise Support
** Available to DCI AWS Customers with Business or Enterprise Support

Service Changes

The Customer and interested parties agree to plan and design any new or changed services. The service design should be agreed with all affected or interested parties prior to development. If any changes are agreed during the course of a project, then the design should be updated and approved. DCI will ensure throughout the design process that the requirements agreed with the Customer include criteria for the quality for the new or changed service.

The new or changed services shall be verified against service acceptance criteria agreed in advance by DCI and interested parties. If the service acceptance criteria are not met, DCI and interested parties shall decide on necessary actions and deployment. When a potential nonconformity to the agreed quality and functional requirements of the service is identified, DCI shall mitigate the risk by changing the design or ensuring the risks are understood and accepted by the interested parties. DCI and the Customer agree that the project shall take into consideration any relevant supplier support agreements, contracts and documented agreements with other parties which can be affected by the changes or additions to the service.

DCI will review the transition with the Customer and interested parties to establish that it is ready for live operation. The resulting decision shall be recorded, together with the Customer's acceptance of the new or changed service into live operation. The transition period shall continue until it is agreed that any remaining activities are part of normal live operation. DCI will record the acceptance by the Customer and interested parties of the new or changed services against agreed acceptance criteria.

Service Removal

DCI and the Customer agree that if an existing service provided by DCI is to be removed, the process shall be planned and documented in a service removal plan. The plan shall include agreed completion criteria for the removal and of the end of DCI's responsibility. DCI will ensure that the details of any outstanding incidents, problems, user requests and requests for change have been agreed with the Customer. Ownership of all data, documentation and system components shall be agreed. If required, arrangements for access to the data or other service components shall be agreed, planned and implemented. Arrangements for archiving, disposal or transfer should also be agreed.

Service removal acceptance criteria shall be documented and agreed with the Customer, including the service management objectives, activities, and outcome of removal of a service. The agreement shall also include how DCI will manage end user data, Customer specific information, service documentation and the affected infrastructure, applications, and licenses.

Service Delivery

DCI and the Customer agree to the services and labor categories in the DCI Service Catalog. The cloud and professional services in the DCI Service Catalog have no dependent service components. DCI and the Customer agree to the service levels defined in this document for each service delivered, unless more specific service levels documented in the performance work statement override these SLAs. DCI and the Customer agree to these SLAs and service targets, workload characteristics and exceptions. DCI has developed, agreed, reviewed and will maintain this agreement to define the activities and interfaces between the two parties. DCI will monitor performance of the Customer against agreed service targets and other agreed commitments in a monthly Service Report.

DCI and the Customer agree to the monthly service reporting as defined in this paragraph. DCI will produce a monthly Service Report that includes service performance against service targets as reported by our Service Desk; relevant information about significant events including all incident types, deployment of new or changed services, and any invocation of the service continuity plan; workload characteristics including volumes and periodic changes in workload; detected nonconformities against the service requirements and their identified causes; trend information; and Customer satisfaction measurements, service complaints and results of the analysis of satisfaction measurements and complaints. The Service Report is available to Customers upon request. DCI, in coordination with the Customer, will make decisions and take actions based on the findings in Service Reports. The agreed actions will be communicated to interested parties.

DCI will assess and document the risks to service continuity and availability of services. Service continuity and availability requirements will be identified and agreed based on the agreed service requirements, the results obtained from business impact analysis exercises, the Customer's business priorities, policies and plans, SLAs, and assessed risks. The agreed requirements shall take into consideration applicable business plans, service requirements, SLAs and risks. DCI will also identify and agree capacity and performance requirements with the Customer and interested parties.

DCI and the Customer agree that a Customer representative and the DCI Service Level Manager are together responsible for the authorization of the service catalog and each SLA is the responsibility of the Customer and service level manager. DCI and the Customer agree that the Customer representative has sufficient authority to agree the definitions of a service in the catalog and the service targets.

The Customer and DCI will document and agree to all capacity requirements and capacity testing requirements. Any required service continuity testing will involve the joint participation of the Customer and DCI, based upon an agreed set of objectives. Authorities and responsibilities required within the service continuity and availability management process should include: the Customer, DCI personnel and interested parties who require access to service continuity and availability management information, participate in testing and agree service continuity requirements. Unless otherwise overridden by additional contract documentation, the Customer and DCI agree that any capacity requirements beyond those inherently provided by Amazon will be initiated by the Customer.

DCI and the Customer will categorize information assets according to value, confidentiality or business impact. For each category, DCI and Customer should define and agree to an acceptable level of risk. Unless explicitly specified elsewhere, the Customer and DCI agree that the services provided by DCI are a low risk to the Customer.

Relationship Management

DCI defines a service complaint as a serious issue submitted in writing by a management representative of the Customer that is beyond the scope of normal day-to-day customer service issues; a service complaint may result from discrimination, employee misconduct, personal injury, property damage, criminal activity, or any other activity or event which may lead to physical, emotional, economic, or reputational injuries. DCI will record, investigate, act upon, report and close service complaints via the DCI Incident Management Procedure includes escalation processes should the Customer does not agree to or accept the proposed actions or resolution. DCI has established a formal review process for recording Customer satisfaction. The Customer agrees to participate in the review process annually, if permitted by corporate policy. The Customer point of contact may determine the appropriate users to participate in the review process. The review shall include a narrative and a rating in the following areas: quality, schedule, cost control, management, and regulatory compliance. The review process shall

include narratives that indicate major strengths and weaknesses in each area and provide the reader with a complete understanding of the DCI's performance. Where possible, customers are encouraged to use the following scale to rate: Exceptional, Very Good, Satisfactory, Marginal, Unsatisfactory. These terms are defined as follows:

Exceptional; Performance meets contractual requirements and exceeds many to the Customer's benefit. The contractual performance of the element or sub-element being evaluated was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective. To justify an Exceptional rating, identify multiple significant events and state how they were of benefit to the Customer. A singular benefit, however, could be of such magnitude that it alone constitutes an Exceptional rating. Also, there should have been NO significant weaknesses identified.

Very Good; Performance meets contractual requirements and exceeds some to the Customer's benefit. The contractual performance of the element or sub-element being evaluated was accomplished with some minor problems for which corrective actions taken by the contractor was effective. To justify a Very Good rating, identify a significant event and state how it was a benefit to the Customer. There should have been no significant weaknesses identified.

Satisfactory; Performance meets contractual requirements. The contractual performance of the element or sub-element contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory. To justify a Satisfactory rating, there should have been only minor problems, or major problems the contractor recovered from without impact to the contract/order. There should have been NO significant weaknesses identified. A fundamental principle of assigning ratings is that contractors will not be evaluated with a rating lower than Satisfactory solely for not performing beyond the requirements of the contract/order.

Marginal; Performance does not meet some contractual requirements. The contractual performance of the element or sub-element being evaluated reflects a serious problem for which the contractor has not yet identified corrective actions. The contractor's proposed actions appear only marginally effective or were not fully implemented. To justify Marginal performance, identify a significant event in each category that the contractor had trouble overcoming and state how it impacted the Customer. A Marginal rating should be supported by referencing the management tool that notified the contractor of the contractual deficiency (e.g., management, quality, safety, or environmental deficiency report or letter).

Unsatisfactory; Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains a serious problem(s) for which the contractor's corrective actions appear or were ineffective. To justify an Unsatisfactory rating, identify multiple significant events in each category that the contractor had trouble overcoming and state how it impacted the Customer. A singular problem, however, could be of such serious magnitude that it alone constitutes an unsatisfactory rating. An Unsatisfactory rating should be supported by referencing the management tools used to notify the contractor of the contractual deficiencies (e.g., management, quality, safety, or environmental deficiency reports, or letters).

Not Applicable; N/A should be used if the ratings are not going to be applied to a particular area.

Control Processes

Change Management

The customer agrees that DCI will review changes for effectiveness and will take actions agreed with interested parties. The customer agrees to the following definitions of change types:

> A ***standard change*** is a pre-authorized change that is low risk, relatively common and follows a procedure or work instruction. A standard change has a priority of Lowest.
>
> A ***normal change*** is any planned service change that is not a standard change or an emergency change A standard change has a priority of Low or Medium.
>
> A ***major change*** is a change that has the potential to have a major impact on services and therefore also on the customer. A major change has a priority of High.
>
> An ***emergency change*** is a change that should be implemented as soon as possible due to impact or urgency. For example, any change that requires immediacy to correct any issue/issue(s) on a business-critical system or to protect the business/organization. An emergency change has a priority of Highest.

Release Management

The Customer agrees that releases will take place on a monthly schedule or as required by the customer. The customer agrees to this release policy and the following definitions of release types:

> A **release** is a collection of one or more new or modified configuration items that are deployed into a live environment. And since a configuration item is any element that needs to be controlled in order to deliver a service, the concept of a release is very broad. It includes not only software releases and document releases but hardware releases as well. A standard release has a priority of Lowest, Low, or Medium.
>
> A **major release** is the introduction of new system, capabilities, or functions into a live environment. A major release has a priority of High.
>
> An **emergency release** is a collection of one or more new or modified configuration items that should be implemented as soon as possible. For example, to resolve a major incident or implement an information security patch. An emergency release has a priority of Highest.

Release acceptance criteria shall be agreed with the Customer and interested parties. The release shall be verified against the agreed acceptance criteria and approved before deployment. Deployment is defined as the action of bringing resources into effective action; deployments generally fall into one of three categories: new installation, replacement, or retirement. Any unsuccessful releases shall be investigated and agreed actions taken.