

**Allegato Tecnico al
Contratto di Appalto di Servizi Informatici tra
ACAM SPA e ACAM CLIENTI SPA**

Allegato A - Servizi

1 Introduzione

1. Il presente allegato descrive i servizi erogati da Acam S.p.A. (“**Acam**” o il “**Fornitore**”) ad Acam Clienti S.p.A. (“**Acam Clienti**” o il “**Cliente**”) nell’ambito del presente contratto (singolarmente il “**Servizio**” e, complessivamente, i “**Servizi**”).
2. Acam fornirà i Servizi in linea con i parametri e i Livelli di Servizio definiti nell’Allegato B e in accordo con i processi di gestione che verranno specificati nel Manuale delle Operazioni.

2 Ambito del Servizio

1. L’ambito dei Servizi è rappresentato dalle seguenti macro-aree:
 - a) Facility Management Service (di seguito FMS) – Allegato A1;
 - b) Application Maintenance Service (di seguito AMS) – Allegato A2;
 - c) Installazione e configurazione del software di cui all’Allegato E;
 - d) Help Desk Service (di seguito Help Desk o Help Desk Service);
 - e) Sicurezza.

3 Installazione e configurazione del software descritto nell’Allegato E

1. Acam si impegna ad installare e a configurare sulla base delle richieste di Acam Clienti il software descritto nell’Allegato E, secondo i corrispettivi indicati nell’Allegato C.
2. Acam concederà ad Acam Clienti la licenza d’uso gratuita, non esclusiva, del predetto software.
3. Relativamente ai software dei quali Acam non è titolare o per i quali non è in grado di fornire il diritto d’uso ad Acam Clienti (si veda tabella E1 ed E2 dell’allegato E) quest’ultima dovrà acquistarne le licenze e/o ogni diritto d’uso che si renda necessario per l’erogazione e la fruizione dei Servizi.

4 Livelli di Gravità e Priorità

4.1 Livelli di Gravità

1. Si riportano nella tabella successiva i Livelli di Gravità (o Severità) presi a riferimento durante la gestione dei Servizi da parte del Fornitore in relazione a chiamate relative a problemi infrastrutturali (FMS) o applicativi (AMS).

2. Il Livello di Gravità verrà definito dall'Help Desk sulla base delle informazioni fornite dall'utente e/o rilevabili dai sistemi.
3. Per i diversi Livelli di Gravità possono essere definiti processi di escalation diversi, atti a soddisfare requisiti espressi in termini di Livelli di Servizio.

GRAVITA' SEVERITA'	Facility Management Service (FMS)	Application Management Service (AMS)
1	Il Servizio non è disponibile. Il problema ha un'alta visibilità e gli utenti non riescono ad operare.	L'intero sistema o un'area funzionale completa (p.e. fatturazione) è bloccata o ferma a causa del problema riscontrato. Le attività di correzione devono essere avviate immediatamente al fine di ripristinare le funzionalità necessarie.
2	La maggior parte degli utenti non può fruire completamente del Servizio. Il problema ha un'alta visibilità. Gli utenti riescono a lavorare in modo degradato e/o hanno limitazioni funzionali.	Il problema causa il blocco delle operazioni. Viene ricondotto a problemi che rallentano o compromettono l'operatività di uno o più utenti finali e potrebbero, se non indirizzati adeguatamente, provocare un grave impatto sulla fornitura dei Servizi. Risultano, altresì, errori che inibiscono un'attività che tuttavia può essere eseguita in altri modi o comunque ritardata.

3	<p>Un singolo utente o comunque una bassa percentuale di utenti è coinvolto.</p> <p>Il problema ha limitata visibilità.</p> <p>Risultano complessivamente funzionalità e performance nella norma ma il Servizio non è pienamente erogato.</p>	<p>Il sistema è impattato in misura limitata dal problema e le ordinarie attività operative possono procedere senza impatti sul business e/o conseguenze legali/fiscali.</p> <p>Le conseguenti attività di correzione saranno prese in carico con la massima tempestività.</p>
---	---	--

4.2 Livelli di Priorità

1. Si riportano nella tabella successiva i Livelli di Priorità assegnati dall'operatore dell'Help Desk in riferimento al problema segnalato.
2. Tale assegnazione non ha nessun impatto sui Livelli di Servizio, ma consente di agevolare la presa in carico da parte dagli enti operativi che intervengono al secondo livello di supporto.
3. Inizialmente tutti i problemi segnalati saranno impostati con priorità 3 (bassa). Nell'ambito del processo di escalation e in presenza di più problemi segnalati, questa assegnazione iniziale potrà essere variata in modo da gestire correttamente la risoluzione dei problemi a seconda della reale priorità di intervento.

PRIORITÀ	DEFINIZIONE
1	ALTA
2	MEDIA
3	BASSA

5 Caratteristiche dell'Help Desk Service

1. Il Fornitore fornisce un servizio di Help Desk per i servizi erogati.

2. Si precisa che potrà accedere all'Help Desk solo il personale del Cliente identificato da un Codice Personale (presente nell'inventario del Fornitore), che sarà utilizzato per verificare la titolarità del chiamante rispetto al servizio richiesto.
3. Il servizio ha le seguenti caratteristiche:
 - a) utilizzo di un applicativo di Trouble Ticketing come strumento per il tracciamento dei ticket;
 - b) produzione di reportistica sul servizio erogato;
 - c) gestione in real time delle code.
4. Le responsabilità nell'ambito Help Desk Service sono le seguenti:

Fornitore:

- a) fornire, programmare e mantenere l'infrastruttura necessaria per l'Help Desk Service;
- b) effettuare l'analisi e una prima determinazione del problema;
- c) verificare ed eventualmente modificare il Livello di Gravità (vedi paragrafo 4.1 Livelli di Gravità) secondo le policy di processo (Problem Management);
- d) assegnare ad ogni segnalazione una priorità secondo le policy di processo;
- e) utilizzare strumenti di controllo remoto (ove previsto) per la risoluzione dei problemi di propria competenza, nel rispetto delle regole di sicurezza;
- f) definire e mantenere i criteri di assegnazione delle priorità e delle procedure di escalation lato Fornitore;
- g) fornire feedback sullo stato della risoluzione dei problemi agli utenti che lo richiedano;
- h) fornire al Cliente un report mensile standard sulle segnalazioni ricevute e gestite dall'Help Desk nel mese precedente. La disponibilità online dei report sarà gestita come Nuovo Servizio;
- i) dare la possibilità al Cliente di monitorare via browser lo stato dei Ticket.

Cliente:

- a) istruire gli utenti in merito alle modalità di contatto dell'Help Desk;

- b) supportare il Fornitore nella definizione delle linee guida delle priorità, severità e delle procedure di escalation, lato Fornitore;
 - c) definire le procedure di escalation, lato Cliente.
5. Il servizio di Help Desk è erogato nella seguente modalità: (i) l'utente apre una richiesta di intervento tramite la piattaforma di Trouble Ticketing; (ii) la richiesta viene presa in carico e gestita dagli operatori del servizio di Help Desk.
6. Le attività sono così svolte:
- a) **apertura della segnalazione:** questa funzione, svolta tramite il sito web Intranet, ha il compito di identificare l'utente, permettere di inserire una descrizione della problematica, inserire il grado di severità e identificare l'apparecchiatura/servizio affetto da anomalia;
 - b) **registrazione della segnalazione:** durante questa fase l'utente inserisce tutti i dati nel sistema informativo, che li renderà disponibili per tutta la durata del processo di gestione della chiamata. Le informazioni minime da inserire sono:
 - i. data e ora di ricezione della chiamata (assegnato automaticamente dal sistema);
 - ii. nome del chiamante, azienda di appartenenza e suo recapito telefonico (assegnato automaticamente dal sistema);
 - iii. descrizione della problematica;
 - iv. severità attribuita;
 - v. priorità attribuita;
 - vi. numero univoco assegnato al problema (assegnato automaticamente dal sistema);
 - vii. nominativo del gruppo/persona a cui è stato assegnato nel caso di non risoluzione immediata (assegnato automaticamente dal sistema).

5.1 Modalità di accesso all'Help Desk Service

- 1. La modalità e le procedure con cui il Cliente potrà avere accesso all'Help Desk del Fornitore saranno descritte e formalizzate all'interno del Manuale delle Operazioni.
- 2. Il Cliente dovrà poter accedere all'Help Desk mediante:
 - a) Web;

- b) Mail;
- c) Telefono (solo in caso di impossibilità ad usare le prime due modalità).

6 Sicurezza

1. Il Fornitore dovrà attenersi ad un Piano Operativo per la Sicurezza nella gestione del servizio.
2. Eventuali misure o interventi che il Fornitore dovrà porre in essere per adeguarsi agli standard minimi di sicurezza previsti dalle vigenti normative saranno a carico del Fornitore stesso.
3. Il Piano Operativo per la Sicurezza definisce i controlli di sicurezza che il Fornitore deve applicare e implementare (“**Controlli di Sicurezza Informatica**”) in relazione ai servizi erogati.
4. Ove non diversamente concordato e fermo restando quanto qui di seguito specificato, il Fornitore tratterà i dati personali adottando le misure di sicurezza previste dal D.lgs. 196/03, limitatamente al trattamento svolto all’interno delle sedi del Fornitore e purché le misure minime da adottare riguardino direttamente attività e strumenti sotto l’esclusivo controllo del Fornitore medesimo.
5. Qualora le operazioni di trattamento dei dati personali non si svolgano in tutto o in parte all’interno di sedi del Fornitore, il Fornitore sarà in ogni caso responsabile di adottare le misure di sicurezza per le attività svolte sotto il suo esclusivo controllo.
6. Le responsabilità in ambito Sicurezza sono le seguenti:

Fornitore:

- a) indicare il Focal Point per la gestione quotidiana della sicurezza;
- b) elaborare, con l’assistenza del Cliente, il documento relativo ai controlli di sicurezza informatica (Fornitore - Cliente) entro 45 (quantacinque) giorni dalla sottoscrizione del contratto di appalto;
- c) concordare, insieme al Cliente, l’efficacia delle politiche e delle procedure di sicurezza e dei piani di adeguamento;
- d) mantenere e aggiornare il documento sui controlli di sicurezza informatica;

e) rivedere le eventuali modifiche richieste dal Cliente alle sue politiche e agli standard di sicurezza e fornire consulenza al Cliente sull'opportunità di effettuare adeguamenti di tali modifiche in termini di:

- i. fattibilità e rischi;
- ii. tempi e costi.

Cliente:

- a) indicare il Focal Point per la sicurezza;
- b) comunicare al Fornitore le proprie politiche e gli standard di sicurezza entro 30 (trenta) giorni dalla data di sottoscrizione del contratto di appalto;
- c) comunicare le procedure di sicurezza agli utenti finali (ad esempio, le procedure di accesso, i requisiti relativi alle password, l'utilizzo di programmi antivirus, le procedure di sicurezza per i dati e le apparecchiature).

6.1 Sicurezza Fisica

- 1. Il Fornitore è responsabile della Sicurezza Fisica dei sistemi.
- 2. In relazione a tutte le apparecchiature informatiche collocate presso il Fornitore saranno, pertanto, assicurate sicurezza fisica e ambientale per la custodia ed il funzionamento delle stesse.
- 3. A tal fine, i Servizi di sicurezza del Fornitore comprendono i seguenti sistemi e servizi ausiliari:
 - a. sistemi anti-intrusione;
 - b. controllo accessi automatizzato;
 - c. sistemi anti-incendio (rilevazione automatica e spegnimento);
 - d. gruppi di continuità elettrica;
 - e. impianto di condizionamento autonomo;
 - f. sistema di supervisione e controllo impianti computerizzato.
- 4. La piena e continuativa funzionalità di tali sistemi deve essere assicurata da specifici piani di manutenzione programmata.
- 5. Le attività di manutenzione straordinaria presuppongono la possibilità per il Fornitore di sospendere l'erogazione dei servizi ausiliari e dei servizi stessi, per il tempo strettamente necessario alle predette attività di manutenzione.

6. La pianificazione della manutenzione straordinaria annuale degli impianti ausiliari deve essere concordata con il Cliente. Questi interventi devono essere pianificati di norma nei giorni festivi e, in ogni caso, devono essere comunicati e concordati con il Cliente.
7. Le responsabilità in ambito Sicurezza Fisica sono le seguenti:

Fornitore:

- a) effettuare con l'assistenza del Cliente entro 60 (sessanta) giorni dalla sottoscrizione del contratto di appalto di servizi un inventario della Baseline (o dei volumi) relativo a supporti fisici (ad esempio, sistemi, supporti di memorizzazione ecc.) la cui responsabilità di sicurezza è di competenza del Fornitore;
- b) effettuare i controlli di sicurezza fisica per l'accesso ai suoi CED;
- c) permettere l'accesso ai CED presso le proprie sedi al solo personale autorizzato;
- d) verificare periodicamente l'inventario dei supporti di memorizzazione e comunicare tempestivamente al Cliente eventuali incongruenze.

Cliente:

- a) assistere il Fornitore nella preparazione dell'inventario della Baseline (o dei volumi) relativo ai supporti fisici la cui responsabilità di sicurezza è di competenza del Fornitore;
- b) proteggere le apparecchiature del Fornitore installate presso le sedi del Cliente e oggetto dei Servizi ed effettuare i controlli di sicurezza fisica. I requisiti minimi di sicurezza fisica che il Cliente deve garantire sono:
 - a. l'area deve avere un responsabile del Cliente ben identificato;
 - b. l'area deve essere chiusa anche quando presidiata;
 - c. l'accesso all'area deve essere limitato al personale autorizzato dal responsabile dell'area medesima;
 - d. il Fornitore ha la possibilità di accettare o rifiutare quanti risultassero inseriti nelle liste d'accesso;
 - e. l'accesso all'area deve essere controllato elettronicamente dai sistemi di accesso;
 - f. l'elenco di quanti autorizzati all'accesso deve essere verificato dal responsabile ogni 6 (sei) mesi;

- g. la documentazione dei controlli e del sistema di gestione verrà fornita al Fornitore direttamente dal responsabile.

6.2 Sicurezza Logica

1. Il Fornitore si impegna ad attuare le misure tecniche di protezione logica nel rispetto delle policy concordate con il Cliente.
2. Nel Piano Operativo per la sicurezza saranno definite le:
 - a. Procedure di Backup;
 - b. Procedure di Disaster/Recovery.
3. Le responsabilità in ambito Sicurezza logica sono le seguenti:

Fornitore:

- a) effettuare entro 60 (sessanta) giorni dalla sottoscrizione del contratto di servizi, con l'assistenza del Cliente, un inventario della Baseline (o dei volumi) degli userid (flussi applicativi, Utenti Finali di S.O) di accesso ai sistemi (sistema operativo, applicazioni, ecc.) la cui responsabilità di sicurezza è di competenza del Fornitore;
- b) identificare i requisiti per la protezione del sistema operativo in modo che possano essere validi a far data dal 1° gennaio 2014;
- c) realizzare le funzioni e le personalizzazioni della logica di controllo degli accessi, concordando i dettagli nel documento sui Controlli di Sicurezza Informatica, al fine di prevenire violazioni di sicurezza intenzionali o accidentali;
- d) realizzare le funzioni e le personalizzazioni di sicurezza del sistema e del software di base, concordando i dettagli nel documento sui Controlli di Sicurezza Informatica.

Cliente:

- a) assistere il Fornitore nella preparazione di un inventario della Baseline (o dei volumi) degli userid (flussi applicativi, Utenti Finali di S.O) di accesso ai sistemi la cui responsabilità di sicurezza è di competenza del Fornitore;
- b) identificare i criteri per la classificazione e il controllo dei suoi dati;
- c) identificare e comunicare i requisiti di protezione e di trattamento di tutti i suoi dati e delle sue risorse;

- d) prevenire per quanto ragionevolmente possibile i tentativi di accesso non autorizzati e mettere in atto le conseguenti azioni correttive necessarie.

6.3 Gestione della Sicurezza dei Server

1. Dove tecnicamente applicabile, la gestione di server e servizi viene erogata con i seguenti controlli di sicurezza:
 - a) Hardening;
 - b) APAR (applicazione delle ultime patch di sicurezza);
 - c) Userid Validation per le utenze del personale del Fornitore;
 - d) Gestione Log sui server (registrazione e conservazione dei tentativi di accesso non autorizzato ai sistemi e ai dati).

6.4 Orario di Servizio

1. Il Fornitore erogherà i Servizi durante l'orario di servizio qui di seguito specificato:

Area	Servizio	Orario di servizio
CUSTOMER CARE CENTER	Help desk primo livello Ricezione e registrazione della richiesta di intervento	Lunedì-Domenica 00:00 – 24:00 CET
	Presidio FMS Analisi e risoluzione problemi infrastrutturali	Allegato A1 - Orario di Servizio
	Presidio AMS Analisi e risoluzione problemi: modulo base e software	Allegato A2 - Orario di Servizio

	applicativi (SAP e altri Software)	
SICUREZZA	Sicurezza fisica	Lunedì-Domenica 00:00 – 24:00 CET
	Sicurezza logica	Lunedì – Giovedì 08:00 – 17:00 CET; Venerdì 08:00 – 12:00 escluso Festività
	Gestione della sicurezza dei Server	Lunedì – Giovedì 08:00 – 17:00 CET; Venerdì 08:00 – 12:00 escluso Festività

7 Documentazione

1. Il Fornitore si impegna a predisporre e aggiornare la documentazione tecnica e operativa relativa alle infrastrutture e ai servizi erogati nell'ambito del contratto di appalto.
2. La documentazione riguarda:
 - a. le scelte tecnologiche operate nell'ambito dei servizi erogati dal Fornitore. A titolo esemplificativo:
 - i. l'architettura Sicurezza;
 - ii. l'architettura di Rete;
 - iii. il documento Piano Operativo per la Sicurezza (come descritto nel presente capitolo);
 - iv. il Manuale delle Operazioni redatto.

Il Cliente ed il Fornitore convengono che nel Manuale delle Operazioni saranno aggiunte/inserite le descrizioni dettagliate delle procedure, delle operazioni e dei processi relativi ai Servizi e che il suddetto manuale verrà mantenuto a cura del Fornitore.

Fino al momento in cui il Fornitore ed il Cliente non avranno completato e approvato il Manuale delle Operazioni, nei limiti dell'applicabilità al nuovo ambiente

operativo delle procedure e dei processi, il Fornitore utilizzerà quanto descritto e definito nell'ambito del presente Allegato.

3. Le responsabilità in ambito Documentazione sono le seguenti:

Fornitore:

- a) creare, aggiornare e mantenere il Manuale delle Operazioni con l'opportuna consulenza del Cliente. Prima di includere nel Manuale delle Operazioni qualsiasi modifica delle responsabilità del Cliente, il Fornitore dovrà ottenere l'approvazione del Cliente;
- b) verificare che la documentazione relativa alle operazioni sia conforme agli standard e alle procedure operative;
- c) distribuire periodicamente al personale designato dal Cliente i comunicati con le informazioni relative alle operazioni e procedure nuove o modificate;
- d) documentare le operazioni relative al software di base e applicativo;
- e) includere nel Manuale delle Operazioni la documentazione fornita dal Cliente, relativamente al Software Applicativo eventualmente utilizzato, non gestito da parte del Fornitore.

Cliente:

- a) fornire tempestivamente documentazione ufficiale relativa agli standard, ai processi e alle procedure operative correlate al Software Applicativo (se non è gestito da parte del Fornitore) eventualmente utilizzato. Il Fornitore includerà tale documentazione, ove esistente, nel Manuale delle Operazioni, apportandovi eventuali opportuni aggiornamenti;
- b) approvare la versione concordata dei documenti.

7.1 Responsabilità del Cliente

- 1. Al fine di garantire i servizi sopra descritti, il Cliente, oltre a quanto già specificato, sarà responsabile di:
 - a) garantire l'accesso nelle proprie sedi al personale per le attività previste;
 - b) rendere disponibili le infrastrutture e impiantistiche necessarie all'installazione del Materiale impiegato per l'erogazione dei Servizi;

- c) garantire la protezione dei Materiali una volta giunti nelle sedi previste;
- d) individuare un Focal Point per ciascuna società identificata nell'Allegato F che figurerà come interfaccia unica ed entry point per le problematiche relative ai servizi qui definiti entro 30 (trenta) giorni dalla data di sottoscrizione del contratto di appalto;
- e) individuare un responsabile da coinvolgere, su richiesta del Fornitore, in caso di interventi on-site.