Attività	*Funzione Responsabile*	*Firma*
Redazione	CED: Andrea NARDI GianLuca GIRANI Pierpaolo SOMMA Progetto Speciale SBE: Anna VALERIANI Area Personale e Organizzazione Antonello GUALANO	
Verifica	Area Personale e Organizzazione Donatella GIROLA	
Verifica	DIRETTORE GENERALE Daniele LUCCI	
Approvazione	AMMINISTRATORE UNICO Antonio MALLAMO	

Indice

Art. 1 - Finalità del Regolamento

1. Il presente "Regolamento Aziendale per la sicurezza e l'utilizzo degli strumenti di informatica individuale", d'ora in avanti "Regolamento", disciplina il corretto utilizzo degli strumenti informatici da parte di tutti i dipendenti di Astral, nonché di tutto il personale che a qualsiasi titolo – quindi a prescindere dal tipo di rapporto e/o utilizzazione con lo stesso intercorrente – presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso le sedi di Astral e che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato e abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche di Astral;
2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche, per "utente" deve intendersi ogni dipendente e lavoratore, così come indicato nel precedente comma, in possesso di specifiche credenziali di autenticazione e/o autorizzazione e che possa essere assegnatario di uno specifico indirizzo di posta elettronica e di un Personal Computer/tablet.

Art. 2 – Attività di conduzione dei sistemi

1. Astral rende noto, con l'approvazione e la diffusione del presente Regolamento, a tutto il personale interessato, che gli Amministratori di Sistema responsabili dei server e della rete, sono autorizzati a compiere interventi sul sistema informatico aziendale, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.);
2. Nel rispetto dei principi di non eccedenza e di pertinenza, di liceità e di correttezza del trattamento(art. 11 D.lgs. 30 giugno 2003, n. 196) i controlli sull'uso di strumenti informatici saranno prioritariamente di tipo aggregato, riferiti all'intera struttura lavorativa aziendale o a sue Aree, quindi di tipo anonimo, e si concluderanno con avvisi generalizzati diretti ai dipendenti della struttura in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base individuale sono giustificati solo qualora le anomalie, nonostante le contromisure adottate in via generale per l'eliminazione delle relative cause, risultino tuttavia persistenti, costituendo un pericolo per la sicurezza del sistema e/o per il regolare funzionamento delle attività di ufficio e/o, ancora, qualora l'utilizzo anomalo degli strumenti informatici, rilevato in sede di controllo, possa integrare eventuali fattispecie di responsabilità sotto il profilo disciplinare, amministrativo-contabile, civile;
3. Il personale di cui al comma 2.1 ha la facoltà di collegarsi e visualizzare da remoto, tramite l'utilizzo di uno specifico software chiamato "Dameware", il desktop delle singole postazioni e del singolo PC/tablet, al fine di garantire l'assistenza tecnica e la normale attività lavorativa, nonché la sicurezza contro virus, spyware, malware etc. previa comunicazione e contestuale accettazione dell'intervento da parte dell'utente interessato. Il suddetto software permette all'utente di monitorare in tempo reale l'attività che gli Amministratori di Sistema responsabili dei server e della rete stanno svolgendo. Di tali connessioni vengono memorizzati i log di accesso.

4. E' in ogni caso fatto divieto di effettuare controlli prolungati, costanti o indiscriminati sull'uso, da parte dei lavoratori, degli strumenti informatici di Astral.

Art. 3 - Utilizzo dei Personal Computer (PC) fissi

1. Il PC è di proprietà aziendale ed è assegnato all'utente esclusivamente come strumento di lavoro; ogni utente è responsabile dell'utilizzo delle dotazioni informatiche assegnate;
2. tutti i PC assegnati devono essere sempre collegati alla rete aziendale, per consentire verifiche di sicurezza ed aggiornamenti. Sono esclusi quelli assegnati dall'azienda per fini diversi, ovvero accompagnati da documento in cui si vieta il collegamento alla rete aziendale stessa;
3. fatto salvo quanto vietato dalla legge, non è consentito all'utente senza preventiva autorizzazione degli Amministratori di Sistema responsabili dei server e della rete:
   - attivare la password d'accensione del PC (BIOS);
   - modificare le caratteristiche hardware e software impostate sul proprio PC;
   - utilizzare Sistemi Operativi Live (da CD, DVD o USB), Sistemi Operativi non autorizzati e software portable (programmi avviabili senza installazione);
   - accedere con diritti amministrativi, locali e di rete;
4. i PC guasti devono essere segnalati agli Amministratori di Sistema responsabili dei server e della rete e non devono essere riparati autonomamente o portati presso strutture esterne all'Azienda;
5. non è consentito l'utilizzo del PC per far uso, archiviare, detenere, duplicare o diffondere in qualunque forma materiali tutelati da diritti d'autore o diritti connessi o sui quali terzi vantano diritti morali e patrimoniali. E' fatto espresso divieto di utilizzo di programmi per il download di materiali protetti da diritto d'autore (Peer to Peer - D.Lgs. n. 68/2003, Legge 22 Aprire 1941 n. 633 e successive modifiche);
6. non è consentito l'utilizzo del PC per far uso, archiviare, detenere o diffondere in qualunque forma materiale pornografico (artt. 600 ter c.p. e 600 quater c.p.). Il divieto comprende anche la semplice navigazione verso siti Internet di tipo pornografico, e comunque verso siti che possano risultare non sicuri;
7. non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004;
8. il PC deve essere spento ogni sera prima di lasciare la postazione di lavoro o in caso di assenze prolungate dalla stessa;
9. le informazioni archiviate informaticamente devono essere esclusivamente quelle consentite dalla legge e necessarie all'attività lavorativa;
10. quando ci si allontana dalla postazione lavorativa è obbligatorio proteggere la stessa bloccandone l'accesso (CRTL+ALT+CANC, selezionando Blocca Computer);
11. è consentito il trasporto di documenti aziendali in formato digitale, al di fuori dell'azienda stessa, solo per fini lavorativi;
12. la gestione locale dei dati aziendali deve essere sostituita dalla gestione centralizzata su server (cartelle condivise sullo share aziendale); eventuali file di lavoro non salvati sul server aziendale sono sotto la completa responsabilità dell'utente; non è consentita l'installazione di programmi diversi da quelli autorizzati dagli Amministratori di Sistema responsabili dei server e della rete;

13. non è consentito, in nessun caso, l'uso di software volti ad aggirare il proxy ed il firewall aziendale per la navigazione in internet;
14. i PC possono essere oggetto di verifica da parte degli Amministratori di Sistema responsabili dei server e della rete, per effettuare controlli a campione ed in caso vengano riscontrate anomalie che compromettano la funzionalità o la sicurezza aziendale, fatta salva la presenza dell'utente. Qualora si riscontrino anomalie ed in caso di assenza dell'utente, il PC verrà scollegato dalla rete, spento e posizionato nel Data Center per le verifiche necessarie;
15. per motivi di sicurezza Aziendale, gli Amministratori di Sistema responsabili dei server e della rete effettueranno ciclicamente delle scansioni per monitorare i processi attivi sui PC, nel rispetto di quanto previsto dall'art. 2 del presente Regolamento;
16. gli Amministratori di Sistema responsabili dei server e della rete possono, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete, dandone preventiva informativa agli interessati;
17. gli Amministratori di Sistema responsabili dei server e della rete possono in qualunque momento avviare il PC dell'utente, anche in assenza dello stesso, per aggiornamenti importanti o scansioni di sicurezza effettuate tramite console remota senza, quindi, accedere localmente al PC;
18. le problematiche riscontrate dall'utente che richiedono un intervento da parte degli Amministratori di Sistema responsabili dei server e della rete, devono essere segnalate esclusivamente tramite l'apertura di un Ticket utilizzando il sito web https://helpdesk, attraverso il modulo presente sul sito http://intranet o semplicemente inviando una mail all'indirizzo supporto@astralspa.it;

Art. 4 - Utilizzo di Personal Computer (PC) portatili e tablet

1. L'utente è responsabile del PC portatile/tablet assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro;
2. Ai PC portatili/tablet si applicano le regole di utilizzo previste per l'utilizzo dei PC fissi (articolo 3) con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna;
3. il PC portatile/tablet deve essere utilizzato solo per il lavoro aziendale e non deve essere inserito in altre reti;
4. i PC portatili/tablet utilizzati all'esterno (convegni, visite in Azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto;
5. il PC portatile/tablet non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari;
6. è vietato utilizzare abbonamenti Internet privati (modem, cellulari, chiavette usb, sim dati) per collegamenti alla rete.

Art. 5 - Utilizzo della rete aziendale

1. L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password);

2. è vietato:
   - utilizzare la rete aziendale per fini non lavorativi;
   - connettere in rete PC o qualsiasi altra apparecchiatura non aziendale;
   - condividere cartelle in rete per uso privato;
3. il monitoraggio di ciò che transita in rete è consentito solo agli Amministratori di Sistema responsabili dei server e della rete.

Art. 6 - Gestione delle Password

1. Tutte le password devono essere complesse e composte da minimo 8 caratteri alfanumerici e non devono contenere riferimenti riconducibili all'incaricato;
2. la password scade ogni 60 giorni e dovrà essere rinnovata. La nuova password dovrà essere diversa dalle 5 precedenti;
3. la richiesta di cambio password da parte dell'utente deve essere presentata esclusivamente dal diretto interessato;
4. è tassativamente vietato l'utilizzo di software atti a trovare le password locali e di rete;
5. l'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione;
6. l'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima;
7. la password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.

Art. 7 - Legittimazione preventiva per l'accesso ai sistemi informatici

1. In caso di mancata osservanza della disposizione di cui al comma 12 dell'art. 3 del presente regolamento e, congiuntamente, in caso di prolungata assenza o impedimento dell'utente incaricato al trattamento dei dati, gli Amministratori di sistema, su richiesta scritta del Responsabile del Trattamento dei dati, potranno accedere ai sistemi informatici dell'incaricato stesso e ai relativi dati in essi contenuti. Al termine della procedura sopra indicata gli Amministratori di sistema provvederanno ad assegnare una nuova password e a bloccare l'account dell'utente incaricato fino al suo rientro in azienda o al sorgere di nuove esigenze da parte del Titolare del trattamento dei dati o del Responsabile.
2. L'accesso ai sistemi informatici e l'utilizzo dei dati contenuti deve, comunque, rispettare i principi di non eccedenza e pertinenza del trattamento dei dati ed è strettamente limitato alle necessità lavorative espresse dal Responsabile del trattamento dei dati.

Art. 8 - Uso della posta elettronica

1. La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro e non deve essere usata per fini privati. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e di qualsiasi attività riconducibile all'uso dell'Account Utente;

2. ogni Account Utente deve essere adeguatamente custodito dall'utente per evitare usi non autorizzati dei servizi da parte di terzi;
3. non è consentito trasmettere o diffondere contenuti che siano illeciti, dannosi, minatori, abusivi, molesti, diffamatori e/o calunniosi, volgari, osceni, lesivi della privacy altrui, razzisti, classisti o comunque reprensibili;
4. non è consentito trasmettere o diffondere un contenuto che comporti la violazione di brevetti, marchi, segreti, diritti di autore o altri diritti di proprietà industriale e/o intellettuale di terzi soggetti;
5. nel caso di messaggi insoliti, mittenti sconosciuti o di messaggi provenienti da mittenti conosciuti ma contenenti allegati sospetti (file con estensione .exe .scr .pif .bat .cmd etc.) è opportuno avvisare gli Amministratori di Sistema responsabili dei server e della rete;
6. nel caso in cui si debba inviare un documento all'esterno dell'Azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf);
7. l'iscrizione a "mailing list" su internet è concessa solo per motivi professionali e previa verifica dell'affidabilità del sito;
8. la casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
9. la dimensione degli allegati non deve mai superare i 5 MB. Per allegati di maggiori dimensioni si dovrà utilizzare il sistema Cloud aziendale;
10. è obbligatorio controllare gli allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti);
11. l'utente può fare una copia dell'archivio di posta (file PST) su uno spazio personale messo a disposizione dall'azienda, con le stesse modalità previste dal comma 8 del presente articolo (vedi procedura di salvataggio sull'intranet aziendale). Ogni archivio di posta (file PST) mantenuto solo in locale sui PC è sotto la completa responsabilità dell'utente;
12. le caselle di posta generiche (es. info@astralspa.it) devono essere usate solo in ricezione;
13. in caso di cessazione del rapporto lavorativo, l'account e l'accesso alla casella di posta, verranno immediatamente disattivati dagli Amministratori di Sistema dei server e della rete;
14. sarà cura dell'utente fare in modo che i documenti necessari al corretto svolgimento dell'attività aziendale, siano messi a disposizione dell'azienda che dovrà poterne disporre anche dopo l'interruzione del rapporto lavorativo;
15. i dati contenuti nelle caselle di posta e le copie dell'archivio di posta, eventualmente salvate sul sever, con le modalità indicate dal comma 11 del presente articolo, vengono conservati per un periodo pari a 12 mesi, in ottemperanza ai principi di necessità, pertinenza e non eccedenza. Tali dati potranno essere utilizzati al solo scopo di recuperarare, nel caso l'utente non abbia seguito le disposizioni del comma precedente, documenti indispensabili allo svolgimento dell'attività aziendale, ovvero allo scopo di tutelare diritti in sede giudiziaria. Al termine del periodo su indicato l'account, la casella di posta ed eventuali archivi, verranno cancellati;
16. il recupero dei dati di cui al comma precedente potrà essere effettuato esclusivamente dagli Amministratori di Sistema dei server e della rete, su formale richiesta del Titolare del trattamento dei dati;

17. il periodo di conservazione di cui al punto 15 potrà essere esteso, fino a cessazione dell'esigenza, su esplicita disposizione del Titolare del trattamento dei dati, ove la documentazione ed i dati d'interesse risultino necessari per garantire continuità operativa e tutela del patrimonio aziendale ovvero per altre finalità espressamente dichiarate dal Titolare, nel rispetto dei principi di cui agli artt. 2, comma 2 e 11, comma 1 del D. l.vo 30 giugno 2003, n. 196.

Art. 9 - Uso della rete Internet e dei relativi servizi

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa;
2. non possono essere utilizzati collegamenti privati (modem, cellulari, chiavette usb, sim dati) per il collegamento ad internet;
3. è vietato l'accesso a siti di tipo pornografico o con contenuti vietati dalla legge;
4. è vietato scaricare, salvo specifiche autorizzazioni, file o software tutelati da diritti d'autore o diritti connessi.

Art. 10 - Uso dei documenti aziendali

1. Al fine di tutelare la sicurezza e la privacy aziendale, è vietato usare sistemi cloud non autorizzati (Dropbox, Sugarsync, Microsoft One Drive, Google Drive, etc.) per copiare documenti aziendali. Ciò è possibile solo sullo spazio Cloud di Astral o eventualmente su uno spazio messo a dispozione da Lazio Crea o Regione Lazio.
2. ogni utente che avesse la necessità di fornire documenti aziendali a società esterne di consulenza, deve evitare tassativamente di inviarli su sistemi cloud non autorizzati (vedi comma precedente);
3. i documenti aziendali possono essere scambiati via mail solo con soggetti autorizzati da Astral, in virtù di rapporti con l'azienda, e devono riguardare attività per le quali i soggetti siano competenti, in virtù di tale rapporto;
4. la posta elettronica potrà essere configurata solo su dispositivi mobili forniti dall'Azienda o autorizzati dalla stessa.

Art. 11 – Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD, supporti USB, etc.) contenenti dati personali nonché informazioni costituenti know-how dell'amministrazione, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun utente dovrà contattare gli Amministratori di Sistema dei server e della rete e seguire le istruzioni da questi impartite;
3. In ogni caso i supporti magnetici contenenti dati personali devono essere dagli utenti adeguatamente custoditi in armadi chiusi o, comunque, in luoghi non accessibili a terzi;
4. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti;

Art. 12 - Criteri e modalità di backup e ripristino dei dati

1. Il sistema di backup consiste in uno Storage e una unità esterna a nastro IBM TS3100 con un drive LTO6 FC;
2. viene effettuato un backup del server di File Sharing tutti i giorni con metodo incrementale;
3. viene effettuato un backup dei File System dei server virtuali tutti i giorni con metodo incrementale;
4. vengono effettuati i backup completi dei server virtuali con cadenza settimanale, mensile o trimestrale a seconda del server;
5. tutti i backup vengono salvati su storage e settimanalmente su nastri LTO6 custoditi in cassaforte ignifuga;

Art. 13 - Protezione antivirus, firewall e sicurezza

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..);
2. ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale (vedi procedura di controllo sull'intranet aziendale);
3. nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso spegnendo il computer segnalando immediatamente l'accaduto agli Amministratori di Sistema responsabili dei server e della rete;
4. ogni dispositivo non aziendale (chiavetta usb, hard disk usb, ecc.) dovrà essere verificato e autorizzato da parte degli Amministratori di Sistema responsabili dei server e della rete prima del suo utilizzo;
5. l'Azienda è protetta da un firewall centralizzato Watchguard ridondato;
6. il firewall ha una licenza "Content Filter" aggiornata che blocca, tramite DataBase esterno, la navigazione sui siti non consentiti dall'Azienda e il download dei file potenzialmente pericolosi in quanto possibili portatori di virus;
7. ogni eventuale altra linea di collegamento ad internet, dovrà essere attestata nel Data Center Astral. Di conseguenza sarà amministrata e messa in sicurezza dagli Amministratori di Sistema responsabili dei server e della rete;
8. al fine di garantire la sicurezza e l'isolamento, la rete interna è suddivisa in Vlan per i progetti che lo richiedono;
9. per i progetti che lo richiedono, la comunicazioni e lo scambio dati con enti/aziende esterne avviene utilizzando una connessione VPN Branch Office dedicata.

Art. 14 - Interruzione dell'erogazione elettrica

1. In caso di interruzione elettrica un gruppo di continuità sosterrà, per circa 30 minuti, i seguenti apparati:
   a. Server aziendali;
   b. Firewall;
   c. Switch del DataCenter;
   d. Connessione internet.
2. non sono predisposti gruppi di continuità a salvaguardia delle singole postazioni di lavoro.

Art. 15 - Mancata osservanza del presente Regolamento e normative di Legge

1. Normativa di legge:
   - ART. 491-BIS C.P. - Falsità in un documento informatico pubblico o avente efficacia probatoria
   - ART. 615-TER C.P. - Accesso abusivo ad un sistema informatico o telematico
   - ART. 615-QUATER C.P. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
   - ART. 615-QUINQUIES C.P. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
   - ART. 617-QUATER C.P. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
   - ART. 617-QUINQUIES C.P. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
   - ART. 635-BIS C.P. - Danneggiamento di informazioni, dati e programmi informatici
   - ART. 635-TER C.P. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità
   - ART. 635-QUATER C.P. - Danneggiamento di sistemi informatici o telematici
   - ART. 635-QUINQUIES C.P. - Danneggiamento di sistemi informatici o telematici di pubblica utilità
   - ART. 640-QUINQUIES C.P. - Frode informatica del certificatore di firma elettronica

2. Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste dalle leggi.

Art. 16 - Aggiornamento e revisione

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione scritta agli Amministratori di Sistema responsabili dei server e della rete;
2. il presente Regolamento è soggetto a revisione con frequenza annuale e può essere aggiornato in qualsiasi momento.

Art. 17 - Entrata in vigore

1. Il presente Regolamento entra in vigore a decorrere dalla data del 31/03/2017 (Ordine di Servizio n. 22/2017 prot. n. 0008035).