Misure sulla sicurezza delle informazioni e divieto di divulgazione

Il lavoratore che svolge il proprio lavoro in modalità agile e si avvale degli strumenti di dotazione informatica forniti da LAZIOcrea S.p.A. deve:

- seguire le policies e le raccomandazioni emanate da LAZIOcrea e pubblicate sulla intranet aziendale;
- effettuare costantemente gli aggiornamenti in particolare quelli relativi alla sicurezza, all'ultima versione disponibile, di tutti i dispositivi di lavoro connessi in rete;
- limitare, al minimo indispensabile, la condivisione, sui social network, di informazioni inerenti, prettamente, la sfera lavorativa;
- assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme a quanto indicato nelle policy in merito alle password;
- bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico in caso di allontanamento dalla postazione di lavoro;
- prestare particolare attenzione alle URL dei siti web. I siti dannosi possono sembrare identici ad un sito legittimo ma l'URL può utilizzare una variazione nell'ortografia o di un dominio diverso;
- segnalare, prontamente, all'organizzazione eventuali e-mail nelle quali viene riconosciuta la non autenticità;
- collegarsi a dispositivi mobili (pen-drive, hdd-esterno ecc.) unicamente se si riconosce la provenienza (nuovi, già utilizzati o forniti dalla società);
- limitare il più possibile l'utilizzo dei WI-FI pubblici per connettersi alla rete aziendale in quanto facilmente attaccabili,
- lavorare tramite l'utilizzo del canale VPN ("Virtual Private Network");
- effettuare sempre il log-out dai servizi/portali che si è conclusa una sessione lavorativa.

Il lavoratore, inoltre, non deve assolutamente:

- installare software provenienti da fonti/repository non ufficiali soprattutto se si viene sollecitati via e-mail;
- cliccare su link o allegati presenti in e-mail sospette
- utilizzare i dispositivi aziendali per fini privati nonché conservare i dispositivi aziendali in un luogo sicuro, quando gli stessi non sono utilizzati.

(si rinvia al link: https://intranet.laziocrea.it/wp-content/uploads/procedure/Raccomandazioni-SM-e-CyberSecurity.pdf).

LAZIOcrea, a seguito dell'espletamento dell'attività lavorativa in modalità agile, ha predisposto, per i lavoratori sessioni di formazione in materia di cyber security.
Pertanto, i lavoratori devono visionare, utilizzando la piattaforma EDU.LAZIO, le pillole video pubblicate sulla piattaforma stessa, al fine di prendere consapevolezza in ordine alla cyber security.

STANDARD DI SICUREZZA - STRUMENTI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA

Per le Policy e le linee guida di riferimento ed in particolare gli "Standard di sicurezza - Strumenti informatici, di internet e della posta elettronica", si rimanda ai sistemi di gestione aziendali in essere, con particolare attenzione al "*Sistema di gestione per la sicurezza delle informazioni (SGSI)*" disponibile al link *https://intranet.laziocrea.it/sgsi-isoiec-27001/*.

SISTEMA DI AUTENTICAZIONE INFORMATICA

In riferimento al sistema di autenticazione informatica, LAZIOcrea S.p.A. ha adottato delle politiche e delle linee guida aventi come scopo la gestione degli accessi ai sistemi informativi al fine di proteggere le informazioni e/o i dati personali aziendali da accessi e trattamenti non autorizzati. Pertanto, i lavoratori devono rispettare le politiche e le linee guida adottate dalla Società. I lavoratori autorizzati si autenticheranno ai sistemi informativi con le proprie credenziali di autenticazione. Le credenziali di autenticazione saranno assegnate ai lavoratori previa formale richiesta e consistono in un codice per l'identificazione dell'utente (user-id) assegnato ad una parola chiave (password) che dovrà essere custodita dall'incaricato con la massima diligenza affinché la stessa non venga divulgata.

Inoltre, LAZIOcrea, oltre al sistema di identificazione sopra descritto, ha adottato, per alcuni sistemi e per l'accesso tramite Virtual Private Network (VPN), il c.d. Multi Factor Authentication ("MFA") o autenticazione a più fattori. Tale tecnologia permette di riconoscere, attraverso più di due metodi di autenticazione, la persona che effettua l'accesso ad un sistema o ad una applicazione.

Pertanto, il personale di LAZIOcrea che accede ai predetti sistemi dotati di MFA è stato dotato di un sistema di autenticazione a doppio fattore (2FA) per cui l'utente che verrà abilitato ai suddetti sistemi dovrà utilizzare, in aggiunta alle proprie credenziali personali di dominio anche il succitato token.

GESTIONE DELLE PASSWORD

La password personale deve essere composta da almeno dieci caratteri, deve contenere almeno 3 (tre) delle seguenti caratteristiche:

i. almeno un carattere maiuscolo,
ii. almeno un carattere minuscolo,
iii. almeno un carattere numerico,

iv. almeno un carattere speciale non alfabetico (ad es. #, %, !).

- La password non deve contenere riferimenti agevolmente riconducibili all'incaricato, quindi la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la propria data di nascita o quella dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.
- La password personale deve essere nota solo all'utilizzatore e non deve essere comunicata a terzi;
- Non può essere usata una password giù utilizzata nei precedenti 4 (quattro) cambi effettuati.
- Risulta importante curare la conservazione e la segretezza della password evitando di trascriverla su un supporto cartaceo precario e visibile (ad es. post-it);
- La password deve essere modificata, al massimo ogni 90 (novanta) giorni.

Qualora in fase di autenticazione fosse inserita una password errata per 8 (otto) volte consecutive l'utenza verrà bloccata per 15 (quindici) minuti e ciò al fine di scongiurare tentativi di ricerca automatizzata delle password.

Le disposizioni indicate si applicano al personale di LAZIOcrea, sia quando svolge le proprie attività lavorative presso la sede della società (dell'Amministrazione Regionale e/o altre sedi specifiche per il servizio di interesse) e sia quando svolge le proprie attività lavorative in smart working e/o telelavoro.

PROCEDURA DI IDENTIFICAZIONE E GESTIONE DEGLI ACCESSI

Il lavoratore per poter accedere alle informazioni aziendali e/o dati personali deve rispettare quanto indicato nella procedura di autenticazione. La suddetta politica, inoltre, stabilisce le azioni necessarie per assicurare la gestione degli account dei Sistemi Informativi. Difatti, LAZIOcrea, in conformità alla normativa di settore nonché ai Sistemi di Gestione Aziendali in essere, ha adottato, per la gestione degli accessi logici ai sistemi informativi, delle politiche al fine di impedire accessi non autorizzati.

La gestione degli accessi comporta l'applicazione delle cosiddette regole "minime sugli applicativi". Pertanto, ogni utente che accede ai sistemi deve avere una identità univoca, quindi non possono esistere identità ridondanti, duplicate ed inattive. L'accesso alle informazioni e/o ai dati personali è differenziato in base ai ruoli ed agli incarichi ricoperti. Si rinvia al link: *Sistema di gestione per la sicurezza delle informazioni (SGSI)*" disponibile al link *https://intranet.laziocrea.it/sgsi-isoiec-27001/*

UTILIZZO DEI DISPOSITIVI INFORMATICI FORNITI DALL'AZIENDA

Il lavoratore nello svolgimento della propria attività lavorativa si avvale degli strumenti informatici - pc portatili, smartphone, connessione wi-fi, connessione remota ecc. - forniti dall'Azienda. Pertanto, il lavoratore, che è responsabile del dispositivo assegnatogli, deve custodirlo con diligenza al fine di evitare danni o sottrazioni. I lavoratori devono comunicare all'Azienda eventuali guasti e anomalie, così come devono comunicare, tempestivamente, eventuali furti o smarrimenti dei dispositivi forniti dall'Azienda. Contestualmente alla suddetta comunicazione il lavoratore dovrà presentare una denuncia alle forze dell'ordine (commissariati di P.S., Arma dei Carabinieri).

Il lavoratore deve prestare attenzione nella conservazione dei dispositivi a lui assegnati al fine di evitare la presa visione dei dati contenuti nei dispositivi da parte di chiunque. Pertanto, l'eventuale perdita o sottrazione di un dispositivo costituisce un "data-breach" (violazione dei dati personali) o potrebbe costituire un rischio per la conoscibilità a terzi, non autorizzati, dei dati personali e/o di informazioni. Si precisa che la comunicazione all'azienda deve essere effettuata entro 24 ore dal verificarsi dell'evento. Si rinvia al seguente link: https://intranet.laziocrea.it/wp-content/uploads/page/POL_SGSI_A.8.1.3-Politica-uso-strumenti-informatici-rev.-1.0.pdf

POSTA ELETTRONICA E MESSAGGISTICA

La casella di posta elettronica assegnata al lavoratore è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica Aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo i casi di assegnazione di notebook e/o telefoni cellulari ad uso promiscuo. Anche in tali ultimi casi sarà comunque necessario attenersi alle misure di salvaguardia della sicurezza nel trattamento dei dati aziendali. Quindi, a titolo puramente esemplificativo, il lavoratore non potrà utilizzare la posta elettronica per:

- l'invio e/o la ricezione di allegati contenenti filmati o brani musicali (es.mp4) non legati all'attività lavorativa;
- l'invio e/o la ricezione di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list non legate all'attività lavorativa;
- la partecipazione a catene telematiche (o cd. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, il lavoratore deve comunicarlo, immediatamente, all'azienda. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Il lavoratore deve porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). Si rinvia al link seguente riguardante la polita dell'uso degli strumenti informatici da parte dei lavoratori: https://intranet.laziocrea.it/wp-content/uploads/page/POL_SGSI_A.8.1.3-Politica-uso-strumenti-informatici-rev.-1.0.pdf

UTILIZZO E CONSERVAZIONE DEI SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI

IL lavoratore, in ordine all'utilizzo ed alla conservazione dei supporti rimuovibili deve rispettare le seguenti regole:

- i supporti di memorizzazione rimovibili (CD e DVD scrivibili, supporti USB, ecc.), contenenti dati particolari, sensibili, nonché informazioni costituenti know-how aziendale, 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.
- al fine di assicurare la distruzione e/o inutilizzabilità di supporti di memorizzazione rimovibili contenenti dati sensibili, ciascun lavoratore dovrà contattare l'ufficio competente e seguire le istruzioni di asset provisioning. In ogni caso, i supporti di memorizzazione contenenti dati personali specie di natura sensibile devono essere adeguatamente custoditi dagli utenti/personale di LAZIOcrea.
- non è consentito, quando si lavora da remoto e quindi in caso di lavoro agile, portare via dalle sedi aziendali hardware e supporti magnetici, ottici o cartacei, se non preventivamente autorizzati.
- è vietato l'utilizzo di supporti di memorizzazione rimovibili personali. L'utente è responsabile della custodia dei supporti e dei dati personali e/o informazioni aziendali in essi contenuti.
- è vietata l'installazione o l'uso di supporti di memorizzazione rimovibili sulle stazioni di lavoro.

UTILIZZO E REGOLAMENTAZIONE DEL SOFTWARE SULLE POSTAZIONI DI LAVORO LOCALI E REMOTE

In riferimento alla regolamentazione del software sulle postazioni di lavoro tutti i dipendenti di LAZIOcrea sono tenuti a seguire le condizioni di utilizzo del software e il rispetto delle licenze. Laddove le condizioni di licenza di un prodotto presentino delle limitazioni di utilizzo (ad esempio: funzionalità, numero di utilizzatori, modalità di utilizzo, ecc.) l'Azienda provvederà a garantire il corretto rispetto delle condizioni di utilizzo e la corretta formazione agli utilizzatori. LAZIOcrea, inoltre, provvede periodicamente ad effettuare un assessment del prodotto per garantire che i diritti

d'autore e gli accordi di licenza siano rispettati. Solo il software con regolare licenza e in conformità con le policy aziendali può essere utilizzato all'interno dell'azienda. Prima dell'utilizzo di qualsiasi nuovo software, il dipendente deve richiedere istruzioni su eventuali accordi di licenza relativi al software, comprese eventuali restrizioni sull'uso dello stesso. È vietata inoltre la duplicazione non autorizzata di software e/o l'utilizzo di copie non autorizzate.

UTILIZZO DELLA RETE

Per l'accesso alla rete/servizi ciascun lavoratore deve essere in possesso della specifica credenziale di autenticazione. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte dell'Azienda. Tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) sono soggette al salvataggio, pertanto il singolo utente deve provvedere al salvataggio dei dati ivi contenuti. L'azienda, in qualunque momento, in caso di identificazione di file o applicazioni in genere pericolose per la sicurezza della rete e/o dei singoli PC, potrà procedere alla rimozione degli stessi e contestualmente provvederà a comunicare il tutto all'utente incaricato. Con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

PROTEZIONE ANTIVIRUS

Il sistema informatico di LAZIOcrea è protetto da un software antivirus che costantemente viene aggiornato. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dalle regole di cui LAZIOcrea si è dotata: (es. navigazione su siti non sicuri, download di file non autorizzati, etc.). Non possono essere modificate, da parte degli utenti, le impostazioni del software antivirus. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto. Si rinvia al link seguente afferente alla politica dell'uso degli strumenti informatici da parte dei lavoratori:

https://intranet.laziocrea.it/wp-content/uploads/page/POL_SGSI_A.8.1.3-Politica-uso-strumenti-informatici-rev.-1.0.pdf

NAVIGAZIONE IN INTERNET

La postazione di lavoro assegnata al singolo utente ed abilitata alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. Di conseguenza il personale dell'Azienda non può navigare in internet per motivi diversi e non connessi all'attività lavorativa.

Pertanto, il personale dell'Azienda non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware e shareware), nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (es.: filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dall'Azienda.

Inoltre, al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa LAZIOcrea rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico. Il predetto Sistema ha come fine ultimo quello di prevenire determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list. L'eventuale controllo sui file di log non è continuativo. Tali file vengono conservati non oltre 180 giorni solari, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda e per le dovute informazioni da rilasciare alle autorità giudiziarie e alle forze dell'ordine. I file più vecchi di 180 giorni vengono ricoperti. Si rinvia al link seguente afferente alla politica dell'uso degli strumenti informatici da parte dei lavoratori: https://intranet.laziocrea.it/wp-content/uploads/page/POL_SGSI_A.8.1.3-Politica-uso-strumenti-informatici-rev.-1.0.pdf

GESTIONE DEI BUCKUP

Sottolineando che le informazioni e i dati personali presenti in una Azienda sono fondamentali e quindi vanno protette altrettanto importante è il recupero degli stessi. Pertanto, in base a tali principi LAZIOcrea si è dotata di una policy di gestione di backup finalizzata a definire le modalità attraverso le quali effettuare il buckup dei dati. Inoltre, la suddetta policy descrive tutto quanto è necessario affinché, in caso di eventi avversi,

che potrebbero mettere a rischio la sicurezza delle informazioni, sia possibile effettuare il ripristino degli stessi ed effettivamente utilizzabili una volta ripristinati. Per ulteriori indicazioni e precisazioni si rinvia: *https://intranet.laziocrea.it/sgsi-isoiec-27001/*

***

Per tutto quanto non contemplato nel presente allegato si rinvia alle Politiche di sicurezza delle Informazioni nonché ai dettami previsti da Sistema di Gestione di Sicurezza delle Informazioni di cui allo standard internazionale ISO/IEC 27001:2014 pubblicato sulla intranet aziendale nell'apposita sezione dedicata alle politiche: https://www.laziocrea.it/intranet/sgsi-isoiec-27001/.

In caso di discordanza, a seguito di aggiornamenti o revisioni, tra quanto indicato nel presente documento e quanto invece indicato sulla intranet aziendale all'indirizzo sopra citato, prevale quanto previsto e pubblicato nella intranet aziendale.