Premessa

L'azienda ha l'obiettivo ambizioso di estendere all'intero Gruppo la certificazione secondo la Norma ISO-IEC 27001, attinente alla sicurezza dei dati e delle informazioni, aspetto essenziale per mantenere la nostra competitività nel settore in cui operiamo.
La persona incaricata d'implementare a livello di gruppo e gestire nel tempo gli adempimenti normativi è stata individuata in Christian Orlandi (Chief Operating Officer - COO) con l'ausilio dei colleghi delle controllate Xcally e Ingo.
Per conseguire l'obiettivo e consolidare le migliori prassi di sicurezza nelle gestione del dato la Direzione chiede il contributo di tutto il personale che viene invitato a rispettare tassativamente le regole indicate nel presente documento.
Eventuali violazioni potranno prevedere richiami verbali; il reiterarsi del fenomeno potrà portare a richiami scritti e conseguenze disciplinari per la risorsa coinvolta.

Trattamento delle informazioni

Il personale dovrà operare:
- avendo la massima cura nell'assicurare che le operazioni di trattamento dei dati si svolgano con la necessaria diligenza ed attenzione in tutte le fasi del trattamento,
- conformando il proprio comportamento in modo da ridurre al minimo i rischi di:
    - esecuzione di trattamento di dati non corretti,
    - distruzione e/o perdita (anche accidentale) di dati,
    - accesso involontario da parte di terzi ai dati e/o alle informazioni,
    - diffusione/comunicazione di dati errata e/o non autorizzata (anche accidentale),
- evitando l'esecuzione di operazioni di trattamento per finalità non previste tra i compiti assegnati,
- evitando l'esecuzione di operazioni di trattamento non consentite e/o non conformi alle finalità per le quali i dati sono stati raccolti,
- garantendo un comportamento improntato alla massima riservatezza dei dati trattati,
- evitando di comunicare o diffondere a terzi i dati senza preventiva autorizzazione,
- attenendosi ai seguenti principi generali:
    - il trattamento dei dati deve essere effettuato in modo lecito e corretto;
    - i dati devono essere completi, pertinenti ed aggiornati;
    - la condotta tenuta nello svolgimento delle operazioni di trattamento dei dati deve essere orientata alla prevenzione dei rischi che incombono sui dati medesimi.

In particolare, salvo autorizzazione, non si possono divulgare foto, video, o altro materiale multimediale, che riprenda locali aziendali e personale che si trova in azienda, senza l'esplicita autorizzazione dell'azienda stessa e delle persone coinvolte.
È infine fatto divieto di acquisire schermate video legate ad esempio ai dati/programmi che si stanno utilizzando oppure effettuare fotografie dei medesimi.

Trattamento degli asset fisici e relativi servizi (internet, mail, etc.)

Gli asset fisici sono costituiti dagli strumenti di lavoro che l'Organizzazione affida al personale per lo svolgimento esclusivo delle attività professionali; ogni altro utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi straordinari e minacce per la sicurezza.

Al personale viene richiesto di:

- trattare diligentemente gli strumenti di lavoro affidati, preservandone l'integrità,
- attenersi, nei casi previsti, alle indicazioni già documentate nel modulo di assegnazione strumenti aziendali (es. in caso di assegnazione di smartphone aziendali, PC portatili, etc.),
- accedere alla postazione fissa attraverso l'inserimento di credenziali personalizzate (password) nel rispetto delle indicazioni sotto riportate:
    - la password deve prevedere otto caratteri alfanumerici contenenti un numero, una lettera maiuscola, una lettera minuscola,
    - la password non deve prevedere elementi facilmente associabili all'utilizzatore in modo da evitare che sia facilmente individuabile,
    - la password deve essere custodita con diligenza e riservatezza, evitando di comunicarla a colleghi e soggetti terzi o evitando di annotarla in modo incauto (es. su post-it),
    - la password dovrà essere aggiornata con cadenza trimestrale (90 giorni),
- non lasciare la postazione di lavoro incustodita: gli elaboratori assegnati non devono essere accessibili a terzi durante le pause di lavoro. Per evitare che questo aspetto accada sono disponibili sistemi di blocco del terminale, mediante attivazione, dopo un tempo prestabilito di inutilizzo, di uno screensaver automatico disattivabile mediante password,
- non utilizzare memorie esterne (es. dispositivi USB) salvo autorizzazione specifica del COO,
- utilizzare smartphone e tablet impostando i seguenti sistemi di sicurezza:
    - impostazione del PIN (4 caratteri),
    - impostazione della password (6 caratteri) oppure il numero massimo di caratteri previsti dal dispositivo,
    - impronta digitale o riconoscimento facciale per i dispositivi che lo prevedono,
- utilizzare i PC portatili rispettando le medesime regole che governano le postazioni fisse, in particolare custodire in modo protetto l'infrastruttura in caso di fruizione in luogo diverso dalle sedi aziendali (ad es. non abbandonare il PC portatile nella vettura in caso di allontanamento),
- rispettare i criteri di "Clear Desk" – scrivania pulita, al termine della giornata lavorativa posizionare i supporti cartacei temporaneamente utilizzati all'interno di armadi/cassetti con criterio e in modo ordinato. Al momento solo per i dati cartacei sensibili dei dipendenti sono stati previsti accorgimenti di sicurezza addizionali, prevedendone la custodia in armadi con chiusura a chiave,
- rispettare i criteri di "Clear Screen" – schermo pulito, in base ai quali viene richiesto agli operatori di backoffice di salvare i documenti rilevanti su cartelle condivise (e non sul proprio Desktop),
- segnalare tempestivamente al COO il furto, lo smarrimento, il danneggiamento degli asset fisici assegnati, eventuali cali di perfomance relativi ai servizi in uso (internet, accesso software, etc.) nonché qualsiasi alert attivato dai sistemi di difesa informatici per possibile accesso di programmi dannosi. La segnalazione di furto o smarrimento interessa anche eventuali PC privati con uso aziendale, in modo che l'azienda possa tutelarsi da eventuali accessi indesiderati alle applicazioni web che ha messo a disposizione del lavoratore,
- spegnere la postazione al termine della giornata lavorativa.

Inoltre, si ricorda al personale che:

- non è consentito utilizzare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente documento,

- non è consentito l'utilizzo di password e/o credenziali d'accesso senza preventiva autorizzazione,
- non è consentito accedere a risorse di rete interne o esterne senza autorizzazione,
- non è consentito operare violando la riservatezza di altri utenti o di terzi,
- non è consentito agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti,
- non è consentito agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori),
- non è consentito permettere ad altri soggetti trasferimenti non autorizzati d'informazioni (software, etc.),
- non è consentito installare o eseguire deliberatamente o diffondere su qualunque PC e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete stessa,
- non è consentito installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali; gli unici software che l'operatore può utilizzare sono stati preventivamente configurati ed installati dal COO o personale ICT delegato,
- non è consentito cancellare, disinstallare, copiare, asportare deliberatamente programmi software per scopi personali,
- non è consentito installare deliberatamente componenti hardware non compatibili con le attività istituzionali,
- non è consentito rimuovere, modificare, danneggiare deliberatamente o asportare componenti hardware,
- non è consentito utilizzare le risorse hardware e software e i servizi disponibili per scopi personali,
- salvo preventive autorizzazioni, non è consentito l'accesso ad Internet per scopi personali,
- non è consentito monitorare o utilizzare qualunque tipo di sistema informatico o elettronico finalizzato a controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita,
- non è consentito memorizzare archivi con dati personali o sensibili,
- non è consentito utilizzare le caselle di posta elettronica per scopi personali,
- non è consentito utilizzare la posta elettronica utilizzando le credenziali di accesso di altri utenti,
- non è consentito in nessun caso utilizzare la posta elettronica per l'invio/la ricezione di materiale contrario ai principi definiti dalla legge (materiale offensivo e/o oltraggioso),
- non è consentito utilizzare device personali per attività di lavoro, né ivi scaricare programmi, software e strumenti aziendali, né salvare sui medesimi documenti aziendali (file, credenziali, ecc.)
- in caso di assenza del personale le e-mail indirizzate al destinatario assente potranno nell'eventualità essere visionate dal responsabile di reparto solo per consentire la gestione rapida ed efficiente delle richieste di servizio, tutelando la riservatezza del lavoratore assente che verrà ovviamente avvisato del relativo accesso temporaneo.

Infine, per quanto riguarda la documentazione cartacea, prima di gettarla nel cestino della carta è necessario provvedere a renderne non comprensibile il contenuto. A tal fine utilizzare apparati distruggi documenti o altri più banali accorgimenti come, ad esempio, strappare i documenti, isolare il dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli, etc.

Trasferimento delle informazioni

Non sono ammessi e previsti scambi via mail relativamente alle informazioni che interessano la gestione ordinaria delle commesse clienti, salvo casi eccezionali preventivamente autorizzati e che possano pertanto prevedere canali protetti straordinari (es. ambienti SFTP, etc.).

I trasferimenti che interessano documentazione anagrafica o sensibile dei lavoratori dovranno essere veicolati unicamente al consulente del lavoro tramite canali sicuri messi a disposizione direttamente dal fornitore.
L'eventuale spedizione di documenti cartacei dovrà avvenire per mezzo di cartelline o buste non trasparenti per la protezione del contenuto.
I messaggi con valenza legale devono essere preferibilmente (in ragione della valenza e della sensibilità della comunicazione) inviati/ricevuti solo attraverso il canale della Posta Elettronica Certificata (PEC), che garantisce quanto segue:

- la persona che invia una PEC è effettivamente chi dice di essere,
- il messaggio originale non ha subito modifiche,
- la comunicazione è criptata.

Accessi fisici

Ogni dipendente ha in dotazione un badge personale ovvero un QR Code il cui rilascio viene autorizzato dall'ufficio Risorse Umane al momento dell'inserimento in azienda.
Il badge è strettamente personale e come tale non è cedibile a colleghi o soggetti terzi.
Nel momento in cui si dovesse smarrire il badge è compito di ogni lavoratore richiedere all'ufficio Risorse Umane un nuovo dispositivo. Il dispositivo smarrito verrà disattivato. Del pari, l'utilizzo del QR Code è strettamente personale, non è cedibile e deve essere custodito con la diligenza richiesta dal ruolo.

Controlli ammessi

Il COO o personale ICT delegato potrà eseguire controlli casuali finalizzati a verificare il corretto utilizzo della rete e delle postazioni.
I controlli verranno eseguiti nel rispetto della normativa Privacy vigente, dei contratti collettivi e della normativa sindacale in materia: in particolare, le verifiche condotte saranno non invasive, anonime e per aggregazione di dati.

Approvazione del documento

Il presente documento viene approvato in data 8 gennaio 2024 dal COO di gruppo e verrà aggiornato nel momento in cui se ne ravvisi la necessità.