Fonderie Guido Glisenti S.p.A. Rev. del 05/09/2024	**DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI**

A. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento interessa tutti i dipendenti e collaboratori a qualunque titolo di Fonderie Guido Glisenti S.p.A. in possesso di credenziali di autenticazione per l'uso di strumenti elettronici (PC e analoghi), indipendentemente dal livello e/o dal rapporto contrattuale in essere con l'ente.
Nell'ambito del presente documento, il termine collaboratori identifica sia i dipendenti che eventuali altre persone in rapporto di collaborazione, a diverso titolo, con l'ente.

B. RIFERIMENTI NORMATIVI

- Provvedimento del Garante per la Protezione dei Dati Personali: "Lavoro: le linee guida del Garante per posta elettronica e internet" (Registro delle deliberazioni; delib. n. 13 del 01 marzo 2007, pubblicato sulla G.U. n. 58 del 10 marzo 2007)
- Regolamento (EU) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali in vigore dal 25 maggio 2018, nonché alla libera circolazione di tali dati e decreti attuativi (101/2018 e successivi).
- Legge 300 del 20 maggio 1970: "Statuto dei lavoratori"
- Legge 633 del 22 aprile 1941: "Protezione del diritto d'autore" e successive integrazioni e modificazioni

C. GESTIONE DEGLI STRUMENTI ELETTRONICI AZIENDALI

Tutti i beni messi a disposizione da Fonderie Guido Glisenti S.p.A., compresi quindi gli strumenti elettronici quali PC, internet, e-mail, telefono, terminali di produzione, software vari e servizi Cloud, ecc., **sono finalizzati ad un uso connesso all'attività dell'Azienda**.
Il loro utilizzo per finalità personali, limitato ed occasionale, è consentito nel rispetto delle vigenti normative in materia di privacy e di diritto d'autore. La Direzione potrà regolamentare o vietare tale utilizzo qualora il personale non dimostri di applicare spontaneamente la necessaria diligenza e serietà nell'utilizzo personale degli strumenti.
È vietato installare/scaricare di propria iniziativa qualsiasi programma software sul PC (o strumento analogo) dato in uso dall'ente o sulla rete informatica.
È vietato, inoltre, scaricare, copiare o anche solamente conservare sugli strumenti elettronici dati in uso da Fonderie Guido Glisenti S.p.A. o sulla rete, file musicali, film, immagini o altro materiale potenzialmente protetti da diritto d'autore o la cui visione e detenzione risulti vietata per legge.
Il collaboratore deve custodire con cura gli strumenti messi a sua disposizione, anche al fine di evitare manomissioni, danneggiamenti, furti o utilizzi illeciti da parte di terzi non autorizzati. A tal fine, particolare cura deve essere dedicata agli strumenti portatili, utilizzabili anche al di fuori della sede di Fonderie Guido Glisenti S.p.A.

D. NAVIGAZIONE IN INTERNET

Fonderie Guido Glisenti S.p.A., a sua discrezione e comunque qualora il personale non dimostri di applicare spontaneamente la necessaria diligenza e serietà nell'utilizzo personale degli strumenti, si riserva la facoltà di applicare limitazioni alla navigazione internet sul luogo di lavoro, anche tramite l'uso di strumenti di content filtering per:

- limitarla ai siti correlati con le proprie mansioni lavorative; oppure
- impedirla per siti o categorie di siti non autorizzati; oppure
- impedirla totalmente.
- Inserire controlli specifici e mirati nel rispetto della normativa vigente e statuto dei lavoratori
- Nel caso sia necessario per l'Azienda effettuare indagini finalizzate all'individuazione di attività dannose per l'Azienda stessa, possono essere temporaneamente attivati controlli specifici, sempre nei limiti previsti dalla normativa vigente.

Tali limitazioni possono essere attivate per singoli utenti o per gruppi omogenei di utenti (ad es. per ruolo, responsabilità o area di appartenenza). E' vietato qualunque utilizzo dell'accesso alla rete internet per fini personali e comunque l'utilizzo dei contenuti in rete deve sempre essere coerente con le finalità aziendali ed adottando tutte le cautele necessarie a garantire l'integrità del sistema informativo.

E. CONTROLLI SPECIFICI TEMPORANEI

Fonderie Guido Glisenti S.p.A., nel caso sia necessario per l'Azienda effettuare indagini finalizzate all'individuazione di attività dannose per l'Azienda stessa, possono essere temporaneamente attivati controlli specifici, sempre nei limiti previsti dalla normativa vigente.
Tali indagini possono essere attivate per singoli utenti o per gruppi omogenei di utenti (ad es. per ruolo, responsabilità o area di appartenenza) e possono comportare l'utilizzo di strumenti informatici esistenti o l'utilizzo di apparati/software specifici oltre che la registrazione di eventi o audio, limitatamente al periodo necessario allo svolgimento dell'indagine interna.

F. UTILIZZO DELLA POSTA ELETTRONICA

L'utilizzo della casella di posta elettronica assegnata deve avvenire nel rispetto dei principi sopra enunciati.
In caso di assenza, programmata o improvvisa, di eventuali persone dotate di indirizzi di posta elettronica nominale, nel rispetto dei diritti di riservatezza e al fine di garantire le normali attività aziendali vengono adottate le seguenti misure tecnico/organizzative:

- **assenza programmata**: va attivato, da parte del destinatario delle e-mail, la delega all'utilizzo della cartella "posta in arrivo" delle mail ad altro incaricato;
- **assenza improvvisa o cessazione del rapporto di lavoro o collaborazione:** al fine di garantire la continuità lavorativa, il Responsabile del trattamento accede al servizio cambiando la password dell'utente e, dopo aver verificato l'assenza di comunicazioni rilevanti per l'azienda, effettua un'esportazione dei contenuti della casella postale e successivamente elimina la casella postale o predispone un risponditore (rifiutando nuovi messaggi email)

Si evidenzia che:

- Particolare attenzione va prestata alla tutela della password, soprattutto nel caso non sia previsto un sistema di doppia autenticazione (ad esempio con password e SMS o token via APP). La password non va comunicata a nessuna persona o società e non deve essere salvata in forma cartacea e/o elettronica. L'Azienda si riserva il diritto di cambiare la password di accesso alla posta elettronica dell'utente per esigenze aziendali e nel caso sia necessario accedere alla casella postale in mancanza dell'utente. La nuova password verrà successivamente comunicata all'utente che provvederà a cambiarla al primo accesso. Nel caso vi sia il dubbio, anche minimo, che la password sia stata trafugata o disponibile a terzi, l'utente deve provvedere a cambiarle immediatamente comunicando all'azienda la possibile violazione dell'accesso alla propria casella postale.
- Particolare attenzione va prestata anche alle mail ricevute, cercando di verificare nei limiti del possibile la veridicità del mittente (controllando ad esempio che il dominio della mail, ovvero la parte a destra dopo il carattere @ dell'indirizzo di posta, sia quello della società indicata come mittente) ed evitare di procede alla richiesta di operazioni (quali ad esempio l'invito a fornire credenziali) che possono essere pericolose per l'Azienda e al tutela della propria casella postale.
- Verificare la tipologia di allegati eventualmente presenti nella mail. Nel caso di dubbio, anche minimo, sulla tipologia di allegato deve essere avvisato il Titolare del Trattamento o l'amministratore di sistema senza procedere ad aprire l'allegato stesso.

L'azienda si riserva la facoltà di inserite dei controlli automatici che possono limitare l'accesso ai contenuti della casella postale o rifiutando/eliminando in modo automatizzato messaggi email con contenuti potenzialmente dannosi o con provenienza da server non considerati attendibili.

G. UTILIZZO DI TELEFONI AZIENDALI, SIM DATI/VOCE AZIENDALI

Nel caso l'Azienda lo ritenga opportuno, può assegnare uno smartphone e SIM (dati e voce oppure solo dati) al dipendente/collaboratore. L'utilizzo di questi strumenti è soggetto alle regole seguenti:

- Lo smartphone va utilizzato con i dovuti criteri di diligenza e conservazione. Eventuali rotture o guasti dovuti ad un uso improprio o non diligente possono essere sanzionati dall'Azienda,
- L'accesso allo smartphone va protetto con codice di blocco (o altra tecnica utilizzabile con modelli specifici di smartphone).
- Le SIM voce/dati consegnate al dipendente, se non espressamente autorizzato, possono essere utilizzate solo in Unione Europea. Il "roaming dati" va sempre e comunque disattivato ed è espressamente vietato l'utilizzo dello

smartphone, delle chiamate e dei dati al di fuori del territorio dell'Unione Europea. Per eventuali addebiti che l'Azienda dovesse ricevere l'utilizzo di chiamate/dati o altro, l'Azienda si riserva la facoltà di rivalsa, addebitandolo al dipendente/collaboratore stesso.

- Considerata la quantità finita di dati a disposizione dell'azienda ed utilizzabili dallo Smartphone/SIM aziendali, è fatto assoluto divieto di utilizzare le chiamate ed il consumo di dati per attività non autorizzate dall'Azienda. Anche in questo caso l'Azienda si riserva il diritto di rivalsa e riaddebito al dipendente/collaboratore.
- Nel caso la SIM o lo Smartphone vengano smarriti, il dipendente/collaboratore dovrà avvisare immediatamente l'azienda che provvederà al blocco SIM e, ove possibile, al blocco del telefono e alla cancellazione da remoto dei dati contenuti.
- In caso di dimissioni, il dipendente deve restituire lo Smartphone e la SIM. Deve inoltre fornire i codici di sblocco del telefono in modo che quest'ultimo possa essere ripristinato ed eventualmente riassegnato. È assolutamente vietato utilizzare in qualunque forma questi strumenti dopo la cessazione del rapporto di lavoro.

H. USO DELLE CHIAVI E DEI BADGE AZIENDALI SE FORNITI

Ogni autorizzato al trattamento che riceve tali strumenti si impegna, a proteggerli da furto, perdita, danneggiamento e, in ogni caso segnalare al Titolare del trattamento il furto, la perdita o il danneggiamento. È vietato lasciarli in luoghi incustoditi.
L'azienda si riserva la facoltà di disabilitarne l'utilizzo e/o ritirare i mezzi resi disponibili. Tali mezzi, infatti, sono strumenti aziendali messi a disposizione dell'autorizzato al fine di consentirgli lo svolgimento della propria mansione ma, come tutti gli strumenti di lavoro, essi rimangono nella completa e totale disponibilità dell'azienda. Alla cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento.

I. UTILIZZO DEI BYOD (DISPOSITIVI PERSONALI UTILIZZATI A FINI AZIENDALI)

Qualora un autorizzato sia stato espressamente autorizzato dalla società all'utilizzo di dispositivi elettronici personali durante le attività lavorative, occorre che si uniformi alle sottostanti prescrizioni, pena l'applicazione di sanzioni.

- i dati trattati devono risiedere solo sulle infrastrutture informatiche e quindi non è consentito scaricare i dati/file/archivi sui dispositivi personali
- i dati personali degli interessati non devono essere trattati per scopi differenti da quelli per cui sono stati originariamente raccolti e devono essere utilizzati solo per il tempo necessario
- deve essere assolutamente evitata la disseminazione indistinta (ad esempio su più dispositivi) dei dati personali oggetto di trattamento tramite BYOD
- l'accesso ai dispositivi deve essere regolamentato da apposite credenziali (es: password o PIN)
- qualora il dispositivo personale che contiene dati del Titolare del trattamento, fosse perso, smarrito, rubato, fosse oggetto di un accesso improprio o comunque ci siano elementi per immaginare/sospettare che i dati contenuti possano essere, sia pure temporaneamente, resi accessibili a terze parti, l'autorizzato deve informare immediatamente il Titolare del trattamento affinché possa essere valutata la problematica e prese, se del caso le opportune misure. La comunicazione deve essere immediata e non possono esser accettati ritardi
- nel caso in cui il dispositivo mobile del lavoratore sia venduto, ceduto, trasferito, il contenuto deve essere cancellato/anonimizzato in modo irreversibile.

J. UTILIZZO DI SISTEMI CHAT (WHATSAPP O EQUIVALENTI). GESTIONE SOCIAL NETWORK E SIMILARI

Il loro utilizzo, con account aziendale, deve essere limitato esclusivamente alle finalità aziendali, per comunicare con referenti interni all'azienda o con clienti e fornitori. Eventuali informazioni contrattuali o commerciali comunicate a mezzo chat devono poi essere confermate a mezzo mail. L'eventuale utilizzo di portali di social network (vedi Facebook, Instagram, Linkedin o similari) deve essere preventivamente autorizzato dall'azienda, così come i contenuti pubblicati.
L'eventuale invio di informazioni, immagini, video tramite Chat (ad esempio WhatsApp, Telegram o altro) deve sempre essere effettuato solo su autorizzazione del Titolare del Trattamento. Si sottolinea che l'invio di dati tramite questi canali ne determina la possibilità che vengano arbitrariamente diffuse da terzi, causando potenziali danni a persone fisiche o

alla società. In tale contesto è necessario che quanto inviato tramite questi canali contenga informazioni che non possano ledere i diritti e la dignità delle persone fisiche o creare danno a terzi o violare i principi di tutela della protezione industriale (quali ad esempio informazioni su prodotti in fase di sviluppo, attrezzature, tecnologie, ecc.)

K. GESTIONE DELLE PASSWORD

Le password per l'accesso al sistema informativo aziendale, alla mail o ad altri servizi in cloud ed interni all'Azienda, devono essere definite dal singolo incaricato rispettando le seguenti regole:

- devono essere composte da non meno di 8 caratteri o di lunghezza/complessità adeguata alla tipologia dei dati a cui si accede,
- il loro contenuto non deve risultare riconducibile all'incaricato (vanno evitati nomi, date, ecc.),
- devono essere sostituite con cadenza periodica ed a conoscenza solo dell'utente stesso (ad esclusione di servizi condivisi tra più utenti ed autorizzati dall'Azienda)
- Non devono mai essere comunicate a terzi, se non su autorizzazione esplicita dell'Azienda.

Tutti i dispositivi, compresi eventuali smartphone, tablet, ecc. tramite i quali sia possibile accedere a dati aziendali, compresa la casella di posta elettronica, devono essere protetti mediante PIN o sistema equivalente. Va in ogni caso escluso il salvataggio delle password tale da consentire l'accesso diretto alle informazioni.

L. EVENTUALI CONTROLLI

Per esigenze produttive, organizzative o di sicurezza il datore di lavoro si riserva, anche tramite l'ausilio di personale tecnico, la facoltà di effettuare controlli graduali e non sistematici sul corretto utilizzo di internet, posta elettronica, telefono aziendale e altra strumentazione informatica; tali controlli potranno essere effettuati anche al fine della prevenzione da utilizzi illeciti da parte dei collaboratori, che potrebbero essere fonte di responsabilità civile o penale.
I controlli potranno riguardare l'analisi dei log contenenti gli indirizzi internet visitati, gli indirizzi delle e-mail inviate/ricevute, informazioni riconducibili all'attività in fase di verifica, i numeri telefonici chiamati/chiamanti; in ogni caso non verrà analizzato il contenuto ma solo l'indirizzo/numero.
Da quanto detto sopra, i controlli possono essere effettuati per l'esercizio di un diritto in sede giudiziaria, in caso di valida manifestazione di un libero consenso, anche in assenza di consenso per un legittimo interesse al trattamento in applicazione del cosiddetto bilanciamento degli interessi (art. 24. comma 1, lett. g del Codice).
Si precisa che questi controlli non avverranno in modo sistematico e, qualora venissero messi in atto, verranno effettuati nel rispetto dei principi di pertinenza e non eccedenza, nel rispetto della vigente legislazione in materia, con particolare attenzione allo Statuto dei Lavoratori, ed in modo graduale, partendo da dati aggregati per scendere via via nel dettaglio in caso di effettiva necessità.
In caso di infrazioni, potranno venire applicate le sanzioni disciplinari previste dal CCNL di competenza per i dipendenti, e quanto previsto dalla normativa vigente.

M. SMARRIMENTO DI STRUMENTI INFORMATICI E NON

Nel caso si verifichi lo smarrimento di strumentazione informatica (quali ad esempio PC Portatili, smartphone, tablet, ecc.) o non informatici (quali ad esempio documentazione cartacea) che potenzialmente possano contenere dati relativi a persone fisiche o dati protetti dalla proprietà industriale dell'Azienda o dati relativi a tecnologie, prodotti, clienti e fornitori dell'azienda, informazioni di tipo commerciale e tecnico o qualunque informazione riconducibile all'azienda, l'Azienda stessa va immediatamente avvisata in modo che possa valutare le azioni da svolgere o eventuali segnalazioni di Data Breach.

N. ESPORTAZIONE DI DATI AL DI FUORI DEL SISTEMA INFORMATIVO AZIENDALE

È vietato esportare, archiviare, trasportare su supporto fisico o logico dati aziendali di qualunque tipo, se non su esplicita autorizzazione dell'Azienda. Nel caso l'azienda abbia previsto strumenti di virtualizzazione del desktop che permette al dipendente/collaboratore di non utilizzare copie locali di file/archivi/programmi (quali Remote Desktop, Citrix o altro

software similare) tale modalità va sempre usata, in quanto contribuisce alla tutela e sicurezza del dato. È fatto quindi divieto di utilizzare altre modalità di accesso se non espressamente autorizzate dall'Azienda.

O. FOTOGRAGRAFIE E VIDEO

Prima di effettuare fotografie o realizzare video che coinvolgano persone fisiche riconoscibili è necessario verificare che sussista una base giuridica che ne consenta la conservazione, la diffusione o l'utilizzo.
Tra le basi giuridiche consentite si indicano:

- Il consenso della persona fisica ripresa per una determinata situazione o in via più generale per un gruppo di situazioni simili tra di loro;

il principio di proporzionalità, nel caso in cui le riprese risultino assolutamente necessarie alla tutela della salute della persona o in casi di emergenza.

P. AMMINISTRATORI DI SISTEMA

Per lo svolgimento delle attività di gestione e controllo del sistema informativo, Fonderie Guido Glisenti S.p.A. ha affidato ad una persona fisica o società esterna l'incarico di amministratore di sistema, incarico che potrà svolgere avvalendosi del supporto di consulenti esterni.