Regolamento per l'Utilizzo degli Strumenti Informatici Aziendali

(Approvato dal Consiglio di Amministrazione del 19 marzo 2026)

1. Finalità

Il presente Regolamento disciplina l'utilizzo degli strumenti informatici e telematici messi a disposizione da gal del ducato S.Cons. a r.l. (di seguito "Società"), al fine di:

- garantire la sicurezza dei dati e dei sistemi informativi;
- tutelare il patrimonio informativo, con particolare riferimento ai fondi pubblici gestiti;
- assicurare la conformità alle normative vigenti (GDPR, Codice Privacy, D.Lgs. 231/2001, Linee guida ANAC, norme su trasparenza e anticorruzione).

2. Ambito di applicazione

Il Regolamento si applica a:

- dipendenti della Società;
- collaboratori, consulenti, fornitori e soggetti terzi autorizzati all'uso dei sistemi informativi;
- membri degli organi societari che accedono a documenti e piattaforme interne.

Gli strumenti coperti includono:

- computer, notebook, tablet, smartphone aziendali;
- rete aziendale, VPN, firewall, Wi-Fi;
- posta elettronica istituzionale;
- software gestionali, piattaforme di rendicontazione, sistemi di monitoraggio fondi pubblici;
- servizi cloud autorizzati;
- dispositivi di archiviazione.

3. Credenziali e accessi

- Le credenziali sono **personali, non cedibili e non delegabili**.
- Ogni utente è responsabile della custodia delle proprie password.
- È vietata la condivisione di account o l'accesso con credenziali altrui.
- Le password devono rispettare i criteri di complessità definiti dalla Società e devono essere aggiornate periodicamente.
- Gli accessi ai sistemi di gestione dei fondi pubblici sono tracciati e soggetti a monitoraggio.

4. Posta elettronica istituzionale

- La casella e-mail aziendale deve essere utilizzata esclusivamente per finalità lavorative.
- È vietato inviare:

    - contenuti non pertinenti all'attività della Società;
    - dati sensibili o altri documenti societari senza adeguate misure di sicurezza;
    - allegati non autorizzati o potenzialmente dannosi.
- La Società può effettuare controlli nel rispetto della normativa vigente e previa informativa agli utenti.

5. Navigazione Internet

- L'accesso a Internet è consentito per attività lavorative e istituzionali.
- È vietato accedere a siti:
    - illegali o non conformi alla normativa;
    - che possano compromettere la sicurezza informatica;
    - non coerenti con le finalità della Società.
- L'installazione di software non autorizzato è proibita.

6. Sicurezza informatica

- Tutti i dispositivi devono essere protetti da antivirus, firewall e aggiornamenti automatici.
- È vietato collegare dispositivi personali senza autorizzazione (BYOD).
- Qualsiasi sospetto incidente informatico (phishing, malware, accessi anomali) deve essere segnalato immediatamente alla Direzione.
- I sistemi utilizzati devono rispettare standard elevati di sicurezza e tracciabilità.

7. Gestione dei dati e dei documenti

- I dati trattati dalla Società, inclusi quelli relativi ai fondi pubblici, devono essere conservati esclusivamente su sistemi autorizzati.
- È vietato esportare dati su supporti esterni non cifrati o non autorizzati.
- La cancellazione dei dati deve essere autorizzata dalla Direzione.
- Gli utenti devono rispettare il GDPR e le policy interne sulla protezione dei dati personali.

8. Lavoro da remoto

In caso di attività svolta fuori sede:

- l'accesso ai sistemi avviene tramite VPN o strumenti sicuri;
- è obbligatorio utilizzare dispositivi aziendali;
- è vietato utilizzare reti Wi-Fi non protette;
- documenti e materiali relativi a gestione di fondi pubblici non devono essere lasciati incustoditi.

9. Controlli, audit e monitoraggio

La Società può effettuare controlli:

- sui log di accesso ai sistemi informativi;
- sul traffico di rete;
- sull'utilizzo dei dispositivi aziendali.

I controlli avvengono nel rispetto:

- dello Statuto dei Lavoratori (art. 4);
- del GDPR;
- delle Linee guida ANAC e delle norme anticorruzione;
- del Modello 231 adottato dalla Società.

10. Violazioni e sanzioni

Le violazioni del presente Regolamento possono comportare:

- richiami formali;
- sospensione degli accessi ai sistemi;
- provvedimenti disciplinari secondo CCNL applicato;
- responsabilità civile e penale nei casi più gravi;
- segnalazioni agli organismi di controllo previsti dal Modello 231.

11. Entrata in vigore e accettazione

Il presente Regolamento è stato approvato dal Consiglio di Amministrazione della Società e consegnato a tutti gli utenti, che devono dichiarare di averlo letto, compreso e accettato.