Repubblica Italiana



Regione Siciliana
Assessorato Regionale dell'Economia
Autorità Regionale per l'Innovazione Tecnologica

Linee guida per l'utilizzo degli strumenti informatici nel lavoro a distanza

SOMMARIO

1 INTRODUZIONE 3
1.1 Finalità 3
1.2 Ambito di Applicabilità 3
2 RIFERIMENTI 4
2.1 Documenti di Riferimento 4
3 ACRONIMI 5
3.1 Acronimi 5
4 Principi Generali 6
5 Requisiti dei dispositivi informatici 6
6 Obblighi comportamentali dell'utente 6
7 Supporto e segnalazioni incidenti 7
8 Responsabilità e accordo individuale 7
9 Disposizioni finali 7

1 INTRODUZIONE

1.1 Finalità

Le presenti linee guida definiscono gli standard tecnologici, le misure minime di sicurezza e le regole comportamentali che i dipendenti della Regione Siciliana devono osservare nello svolgimento dell'attività lavorativa a distanza, ivi incluse le forme di lavoro agile, telelavoro domiciliare e, ove applicabile, coworking autorizzato.

La finalità è garantire che l'accesso alle risorse della Rete Telematica Regionale Siciliana (RTRS) ed il trattamento dei dati istituzionali avvengano in condizioni coerenti con i requisiti di riservatezza, integrità, disponibilità e resilienza richiesti dalla normativa vigente in materia di protezione dei dati personali e cybersicurezza.

Le misure indicate costituiscono requisiti minimi; in funzione della tipologia di dati trattati, delle applicazioni utilizzate e del profilo di rischio dell'attività, l'Amministrazione potrà prevedere misure ulteriori o restrizioni più rigorose.

1.2 Ambito di Applicabilità

Le presenti linee guida si applicano a tutto il personale che, previa autorizzazione e nei limiti previsti dagli atti organizzativi e dagli accordi individuali applicabili, svolge attività lavorativa a distanza accedendo a sistemi, applicazioni, banche dati, file server, servizi cloud o altri asset informativi dell'Amministrazione regionale.

Le presenti linee guida si applicano a tutti i dispositivi informatici utilizzati per lo svolgimento dell'attività lavorativa a distanza.

2 RIFERIMENTI

2.1 Documenti di Riferimento

Rif.	Titolo
DR-1.	Regolamento (UE) n. 679/2016 (GDPR): Regolamento generale sulla protezione dei dati relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
DR-2.	Direttiva (UE) 2022/2555 (Direttiva NIS2): Relativa a misure per un livello comune elevato di cybersicurezza nell'Unione.
DR-3.	D.Lgs. 7 marzo 2005, n. 82 (CAD): Codice dell'Amministrazione Digitale e successive modifiche e integrazioni.
DR-4.	D.Lgs. 30 giugno 2003, n. 196: Codice in materia di protezione dei dati personali (così come modificato dal D.Lgs. 101/2018).
DR-5.	L. 22 maggio 2017, n. 81: Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato (Legge sul Lavoro Agile).
DR-6	Circolare prot. 4535 del 27/06/2022 (A.R.I.T.) - Politica specifica per il corretto utilizzo delle risorse informatiche aziendali

Tabella 1 - Documenti di Riferimento

3 ACRONIMI

3.1 Acronimi

Vocabolo	Titolo
ACN	Agenzia per la Cybersicurezza Nazionale
A.R.I.T.	Autorità Regionale per l'Innovazione Tecnologica
CSU	Centro Supporto Utenze
DDG	Decreto Dirigente Generale
EDR	Endpoint Detection and Response (Soluzione di sicurezza informatica che monitora i dispositivi connessi alla rete per rilevare, analizzare e rispondere a minacce informatiche)
GDPR	General Data Protection Regulation (Regolamento UE 2016/679)
ICT	Information and Communication Technology (Tecnologie dell'informazione e della comunicazione)
MFA	Multi-Factor Authentication (Autenticazione a più fattori)
NIS	Network and Information Security (Sicurezza delle reti e delle informazioni)
OTP	One-Time Password (Codice di accesso monouso)
RTRS	Rete Telematica Regionale Siciliana (indicata come Rete Regionale)
SIDI	Sicilia Digitale S.p.A.
VPN	Virtual Private Network (Rete Privata Virtuale)

Tabella 2 - Acronimi

4 Principi Generali

L'Amministrazione promuove il "*principio di equivalenza tecnologica*": i dispositivi informatici utilizzati per lo svolgimento dell'attività lavorativa a distanza devono offrire un livello di protezione equivalente a quello dei dispositivi informatici disponibili negli uffici regionali.

- **Modalità operativa**: l'utilizzo di dispositivi forniti dall'Amministrazione costituisce la modalità preferenziale di svolgimento del lavoro a distanza;
- **Minimo privilegio**: l'accesso a sistemi e dati deve essere limitato alle sole risorse necessarie allo svolgimento delle mansioni assegnate;
- **Modalità di accesso alla rete:** l'accesso da remoto alla rete RTRS deve avvenire esclusivamente tramite il software client VPN messo a disposizione dall'Amministrazione con autenticazione MFA mediante OTP;
- **Responsabilità dell'utente:** il dipendente è tenuto a custodire dispositivi e credenziali, a rispettare le istruzioni ricevute e a segnalare tempestivamente eventi anomali o incidenti;
- **Protezione dei dati:** i dati istituzionali devono essere trattati esclusivamente con strumenti e modalità autorizzati dall'Amministrazione.

5 Requisiti dei dispositivi informatici

I dispositivi informatici utilizzati per lo svolgimento dell'attività lavorativa a distanza devono rispettare i seguenti requisiti:

- Il Sistema operativo deve essere supportato dal produttore, prevedere l'installazione automatica degli aggiornamenti di sicurezza ed avere una licenza valida (commerciale o open-source);
- Il Software Antivirus/Antimalware deve essere attivo, aggiornato ed avere una licenza valida (commerciale o open-source);
- Il Software Client VPN da utilizzare per l'accesso alla rete RTRS deve essere fornito dall'Amministrazione;
- Il disco del dispositivo deve essere cifrato, dove tecnicamente possibile;
- La password di accesso al dispositivo deve essere conforme ai requisiti minimi di complessità.
- Il blocco automatico dello schermo deve essere impostato dopo un periodo di inattività adeguato (fra 1 e 5 minuti);
- I software di terze parti utilizzati per lo svolgimento delle attività lavorative deve devono essere aggiornati e con licenza valida (commerciale o open-source).

6 Obblighi comportamentali dell'utente

Gli obblighi comportamenti dell'utente includono le seguenti responsabilità:

- Utilizzare Password, PIN e sistema di sblocco conformi ai requisiti stabiliti nella politica specifica per il corretto utilizzo delle risorse informatiche aziendali – Rif. DR-6;
- Non effettuare il salvataggio di dati, documenti o copie di lavoro su supporti rimovibili;
- Non utilizzare account di posta elettronica, servizi di archiviazione, strumenti di messaggistica e profili personali (es. account privati di email, cloud storage, chat o videoconferenza) per lo svolgimento di attività istituzionali e per la trasmissione di dati e documenti dell'Amministrazione;
- Non lasciare il dispositivo incustodito o accessibile a terzi;
- Mantenere riservati credenziali e fattori di autenticazione;
- Evitare l'utilizzo di reti Wi-Fi pubbliche o non protette;
- Non stampare documenti contenenti dati istituzionali al di fuori dei locali dell'Amministrazione, salvo autorizzazione;

- Segnalare tempestivamente furto, smarrimento, compromissione, malfunzionamenti anomali o sospetto incidente di sicurezza.

7 Supporto e segnalazioni incidenti

Per eventuali problematiche di assistenza tecnica o segnalazioni di incidenti informatici che possano impedire il normale svolgimento delle proprie attività lavorative a distanza il dipendente dovrà inviare un'email al csu@regione.sicilia.it. Nell'ipotesi in cui non sia possibile accedere alla rete o alla posta elettronica, si dovrà utilizzare il canale telefonico al numero: 091-7077777.

8 Responsabilità e accordo individuale

L'efficacia delle presenti linee guida presuppone che gli obblighi in esso contenuti siano recepiti nell'accordo individuale di lavoro a distanza o negli atti organizzativi equivalenti, con specifica indicazione della dotazione informatica assegnata o autorizzata dell'utente.
Il dipendente è responsabile del rispetto delle istruzioni ricevute e dell'utilizzo corretto degli strumenti assegnati o autorizzati.

9 Disposizioni finali

Le presenti linee guida entrano in vigore dalla data di adozione formale da parte dell'Amministrazione. Eventuali aggiornamenti potranno essere disposti in relazione all'evoluzione normativa, tecnologica, organizzativa o del profilo di rischio.
Per quanto non espressamente disciplinato, si applicano le politiche di sicurezza, le istruzioni operative e le disposizioni organizzative vigenti presso l'Amministrazione regionale.