# Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/2001 adottato da

# Associazione Irrigazione Est Sesia

**(in seguito, per brevità, “Est Sesia” o “AIES” o “l’Associazione” o l’“Ente”)**

## Parte Speciale P07

## Processo Gestione dei Sistemi Informativi

**Finalità**

La presente Parte Speciale ha la finalità di definire i protocolli specifici di comportamento e di controllo che tutti i soggetti coinvolti nell'ambito delle attività "sensibili" previste nel processo "gestione dei sistemi informativi", di seguito "GSI", dovranno seguire al fine di prevenire la commissione dei reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

**Attività sensibili nell'ambito del processo "GSI"**

Le attività sensibili individuate, con riferimento al processo "GSI" sono le seguenti:

1. accesso ai sistemi informatici aziendali o di terze parti, che contengono: (i) informazioni bancarie; (ii) dati di fatturazione o di credito; (iii) dati relativi a pagamenti; (iv) altra documentazione in formato digitale;
2. gestione degli strumenti informatici in dotazione agli utenti (con particolare riguardo alla gestione dei profili di accesso alle apparecchiature informatiche, alla rete ed ai sistemi e all'installazione del software e gestione delle applicazioni esistenti);
3. gestione della sicurezza informatica, dell'infrastruttura informatica e degli strumenti di connettività aziendale (gestione dei back up, gestione del data center environment, ripristino da fallimenti delle operazioni, acquisto di strumenti hardware e software).

**GSI01 - Accesso ai sistemi informatici aziendali o di terze parti, che contengono: (i) informazioni bancarie; (ii) dati di fatturazione o di credito; (iii) dati relativi a pagamenti; (iv) altra documentazione in formato digitale**

Il processo di gestione e assegnazione degli account e degli accessi logici ai sistemi informativi aziendali è formalizzato nelle procedure di seguito elencate e nel "Regolamento interno per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet", che disciplina i comportamenti da adottare nell'ambito dell'accesso ai sistemi informatici e a cui si fa espresso e diretto richiamo nella presente Parte Speciale.

In generale, è previsto un formale sistema di autorizzazioni volto a consentire l'accesso al sistema amministrativo-contabile esclusivamente ai soggetti che per la propria mansione necessitano di tali accessi. Sono inoltre presenti log di registrazione delle attività effettuate da ciascun utente.

*Le Categorie di Reato applicabili*

Sulla base del *control & risk self assessment* svolto, l'attività sensibile risulta potenzialmente rilevante per le seguenti categorie di reato:

| | |
|---|---|
| ***Delitti informatici e trattamento illecito di dati (art. 24-bis)*** | Dipendenti dell'Associazione si introducono abusivamente in sistemi informatici esterni al fine di carpire informazioni che possano procurare un interesse o vantaggio alla Società stessa. |
| ***Reati tributari (art. 25 quinquiesdecies)*** | Anche in concorso con altre funzioni aziendali, gestire abusivamente l'infrastruttura IT al fine di occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi. |

*Protocolli di comportamento e controllo*

Di seguito sono indicati i protocolli definiti relativamente all'attività sensibile individuata.

- Est Sesia si è dotata di un Regolamento volto a disciplinare l'utilizzo degli strumenti informatici, della posta elettronica e di Internet "regolamento interno per l'utilizzo degli strumenti informatici, della posta elettronica e di internet" reso noto a tutti i Dipendenti tramite circolare n. 9 dell'11 ottobre 2021, il cui dettato qui si riassume.
- Ogni richiesta di creazione di utenza, modifica della stessa o sua eliminazione deve essere soggetta ad apposito iter di approvazione e, comunque, devono essere abilitate le funzionalità strettamente necessarie all'esecuzione della mansione associata.
- In sede di creazione/modifica/eliminazione di un'utenza, il GOI provvede a:
  - verificare che la richiesta provenga da soggetto formalmente identificato (e.g. Responsabile diretto) e che sia stata formalmente autorizzata;

- verificare che la profilazione dell'utenza sia conforme alla mansione ricoperta dal destinatario dell'utenza;
- attribuire un codice identificativo univoco (user-id) all'utenza ai fini dell'accesso ad applicazioni ed alla rete internet.

- Il GOI è inoltre responsabile della definizione di criteri e modalità per la creazione delle password di accesso alle reti aziendali, alle applicazioni e indicazione delle scadenze delle stesse.
- Il personale di Est Sesia è responsabile della corretta gestione della propria user-id e della password, sia in termini di divulgazione delle stesse che in termini di aggiornamento e rispetto di tutte le regole definite dal GOI.
- Periodicamente, GOI provvede a verificare che non siano presenti utenze "obsolete" (e.g. a fronte di dimissioni/licenziamenti) e, nel caso si attiva per la loro eliminazione o disabilitazione.
- Tutte le attività effettuate dagli utenti e dagli Amministratori di Sistema sono tracciate in appositi file di log, di cui sono garantite l'integrità e l'immodificabilità.
- Gli utenti già profilati che intendano connettersi da remoto alla rete interna sono in grado di farlo mediante connessione in VPN; laddove tecnicamente possibile, l'accesso in VPN avviene mediante meccanismi di autenticazione basati su strong authentication definiti da parte di GOI.
- Al fine di minimizzare il rischio di accesso non autorizzato alle risorse di rete, la connessione alla rete WLAN è consentita unicamente ai soggetti autorizzati, previa autenticazione mediante l'impiego di un protocollo di sicurezza autorizzato, sicuro e affidabile.

**GSI02 - Gestione degli strumenti informatici in dotazione agli utenti (con particolare riguardo alla gestione dei profili di accesso alle apparecchiature informatiche, alla rete ed ai sistemi e all'installazione del software e gestione delle applicazioni esistenti)**

Il processo di gestione e assegnazione degli account e degli accessi logici ai sistemi informativi aziendali è formalizzato nelle procedure operative di seguito elencate e nel "Regolamento interno per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet", che disciplina i comportamenti da adottare nell'ambito dell'accesso ai sistemi informatici e a cui si fa espresso e diretto richiamo nella presente Parte Speciale.

*Le Categorie di Reato applicabili*

Sulla base del *control & risk self assessment* svolto, l'attività sensibile risulta potenzialmente rilevante per le seguenti categorie di reato:

| | |
|---|---|
| ***Reati tributari (art. 25 quinquiesdecies)*** | Dipendenti dell'Associazione si introducono abusivamente in sistemi informatici esterni al fine di carpire informazioni che possano procurare un interesse o vantaggio alla Società stessa. |
| ***Delitti in materia di protezione del diritto d'autore (art. 25 novies)*** | Utilizzo da parte dell'Ente di programmi senza licenza o uso di immagini o pubblicazioni coperte da diritto d'autore. |

*Protocolli di comportamento e controllo*

Si fa riferimento alle procedure allegate.

- Procedura_Registrazione_Deregistrazione_Accessi Est Sesia;
- Procedura_Provisioning_Accessi App;
- Procedura_Assegnazione Asset.

Di seguito sono riassunti i protocolli definiti relativamente all'attività sensibile individuata.

- È responsabilità di GOI garantire una corretta gestione delle modalità di accesso (sia fisico sia informatico) di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, delle modalità di accesso (sia fisico sia informatico) di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.

- GOI è responsabile della gestione dei rapporti con i terzi (Responsabile CED) in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. In tale ambito GOI è inoltre incaricato di monitorare l'operato del terzo e di garantire il rispetto del corretto trattamento dei dati da questo acquisiti.
  I soggetti terzi che devono accedere alla rete aziendale e/o solo a determinati server, per interventi di assistenza e supporto tecnico, sono nominati "Responsabile del trattamento" con apposita lettera di nomina firmata da entrambe le parti, Est Sesia e fornitore di servizi, in fase di sottoscrizione del contratto e vengono catalogati nel Sistema di accesso "Guacamole" che è utilizzato come strumento di accesso remoto con autenticazione criptata su protocollo HTTPS. Le password di accesso vengono create e assegnate dai GOI in fase di attribuzione utenza.
  La password può essere modificata dal possessore delle credenziali di accesso.
- In generale, il personale di Est Sesia è diffidato a effettuare copie non specificatamente autorizzate di dati sensibili e di software protetti da licenza. (Ripreso da GSI03)
- GOI ha implementato una struttura informativa e di controllo IT volta a monitorare e limitare l'accesso alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi ed alle applicazioni; in particolare, GOI ha definito quanto segue:
  - obbligo di autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  - assegnazione agli utenti di profili di accesso specifici e selettivi a funzioni e dati che lo richiedono;
  - accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete
  - obbligo di custodia dei dispositivi di memorizzazione (ad esempio chiavi USB, CD, hard disk esterni) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
  - regole di assegnazione e gestione degli apparati abilitanti l'accesso personale ai sistemi e alle applicazioni (ad esempio, dispositivi di autenticazione o di firma).

Con riferimento alle regole adottate da Est Sesia per l'attribuzione e relativa gestione delle utilities (sia informatiche che non), si rimanda a quanto disciplinato all'interno dell'attività sensibile "Assegnazione e gestione dei beni strumentali e delle utilità aziendali (es. personal computer, carte di credito, cellulari, autovetture, ecc.)", a cui si fa espresso riferimento.

**GSI03 - Gestione della sicurezza informatica, dell'infrastruttura informatica e degli strumenti di connettività aziendale (gestione dei back up, gestione del data center environment, ripristino da fallimenti delle operazioni, acquisto di strumenti hardware e software)**

Al fine di garantire un agevole e strutturato sistema di gestione della sicurezza informatica, Est Sesia si è dotata, per il tramite del proprio GSI, di un sistema di ticketing in grado di supportare la gestione degli "incidenti di sicurezza informatica". Tale sistema di ticketing provvede a classificare, prioritizzare e a protocollare gli errori riscontrati, anche al fine di garantire tracciabilità degli interventi e degli incidenti riscontrati.
Inoltre, al fine di garantire la business continuity, il GSI ha implementato logiche di back-up delle informazioni e delle scritture obbligatorie, che in particolare:

- mantiene le copie di back-up in luoghi sufficientemente distanti al fine di prevenire il rischio di perdita derivante da calamità o altri rischi "territoriali";
- effettua test sul ripristino delle scritture contabili obbligatorie;
- esegue un'attività di monitoraggio sull'esito dei backup e, qualora vi fossero riscontrate anomalie, vengono prese in carico e risolte tempestivamente.

All'atto della configurazione di un nuovo terminale (o altra apparecchiatura hardware), GOI provvede ad installare antivirus e firewall. Periodicamente viene richiesto ai dipendenti utilizzatori del terminale/hardware di effettuare gli aggiornamenti alla versione di antivirus e firewall più aggiornati. Gli eventuali "mancati" aggiornamenti vengono monitorati da parte di GOI che eventualmente attua i dovuti correttivi.
Al fine di garantire l'impossibilità di accesso ad informazioni riservate e/o intrusioni non autorizzate, la rete aziendale risulta essere segregata in due ambienti distinti e non connessi tra loro: un ambiente è riservato ai dipendenti dell'Associazione ed alle apparecchiature abilitate; un altro ambiente è invece reso disponibile ai

soggetti esterni. Inoltre, per le sedi decentrate (e comunque anche per l'esecuzione di attività in modalità "smart-working") l'accesso alla rete aziendale (e relativa compartimentazione) è attuabile per il tramite di VPN. Con particolare riferimento invece all'introduzione all'interno del sistema dell'Associazione di hardware e software "nuovi", si segnala che in generale Est Sesia procede, nei casi di sostituzione delle postazioni obsolete che non richiedono particolari caratteristiche hardware, allo scouting di soluzioni "ricondizionate" e, comunque, prima del loro inserimento, il prodotto viene testato e verificato da parte del GOI, al fine di precludere ogni eventuale rischio per Est Sesia. Inoltre, in caso di asset informatici ad alto valore, l'inserimento avviene sempre per il tramite di gara di acquisto che vede il coinvolgimento di GOI per l'esecuzione dei controlli di adeguatezza previsti.

*Le Categorie di Reato applicabili*

Sulla base del *control & risk self assessment* svolto, l'attività sensibile risulta potenzialmente rilevante per le seguenti categorie di reato:

| | |
|---|---|
| ***Delitti informatici e trattamento illecito di dati (art. 24-bis)*** | Dipendenti dell'Associazione si introducono abusivamente in sistemi informatici esterni al fine di carpire informazioni che possano procurare un interesse o vantaggio all'Associazione stessa. |
| ***Reati tributari (art. 25 quinquiesdecies)*** | Anche in concorso con altre funzioni aziendali, gestire abusivamente l'infrastruttura IT al fine di occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi. |

*Protocolli di comportamento e controllo*

Di seguito sono indicati i protocolli definiti relativamente all'attività sensibile individuata.

- In caso di smarrimento di hardware di proprietà di Est Sesia, il dipendente assegnatario di tale hardware deve effettuare segnalazione a GOI, il quale si deve attivare per limitare le eventuali perdite di informazioni o la possibilità di intrusione non autorizzata per il tramite di tale hardware.
- In generale, il personale di Est Sesia è diffidato a effettuare copie non specificatamente autorizzate di dati sensibili e di software protetti da licenza.
- GOI ha provveduto ad implementare un inventario dei software, delle banche dati e dei contenuti protetti dal diritto d'autore (o copyright), comprensivo delle informazioni sulle relative licenze d'uso, al fine di attuare attività di monitoraggio sul rispetto delle condizioni contrattuali.
- GSI ha implementato logiche di back-up al fine di garantire l'accessibilità ed il ripristino dei dati chiave in caso di disastro o di incidente informatico; in particolare:
  - le copie di back-up sono mantenute in luoghi sufficientemente distanti al fine di prevenire il rischio di perdita derivante da calamità o altri rischi "territoriali";
  - periodicamente vengono effettui test sul ripristino delle scritture contabili obbligatorie;
  - è presente un'attività di monitoraggio sull'esito dei backup e, qualora vi fossero riscontrate anomalie, vengono prese in carico e risolte tempestivamente da parte di GOI o di consulente informatico incaricato.
- GOI è responsabile del monitoraggio del corretto funzionamento di antivirus (a livello di installazione e rilascio di eventuali aggiornamenti) al fine di prevenire eventuali incidenti informatici. I firewall sono gestiti e configurati su richiesta dal CSI per la rete internet e di gestione domini e da Vodafone per la rete MPLS.
- In sede di acquisto di hardware e software, Est Sesia deve rispettare quanto previsto nell'ambito del processo "Gestione degli acquisti di beni, servizi e consulenze", con la particolarità che deve essere contemplato il coinvolgimento di GOI per il rilascio di un parere esplicito preliminarmente all'esecuzione dell'acquisto.

**“PROCEDURA PER LA REGISTRAZIONE O DE-REGISTRAZIONE DEGLI ACCESSI”**

Sommario

# 1. SCOPO, AMBITO DI APPLICAZIONE E DESTINATARI

## 1.1. SCOPO

Lo scopo del presente documento è quello di illustrare il processo di registrazione o de-registrazione con attivazione delle credenziali per accedere alla postazione di lavoro. L'accesso agli applicativi, l'eventuale necessità di abilitare indirizzi mail, varie ed eventuali seguiranno apposita procedura.

Il fine è quello di regolamentare con un processo chiaro e condiviso le operazioni, le responsabilità e i ruoli di tutti gli attori coinvolti nel processo di registrazione o de-registrazione degli utenti, così da garantire che non vi siano accessi alla rete aziendale non autorizzati.

## 1.2. AMBITO DI APPLICAZIONE

La procedura si applica nei seguenti casi:

- ASSUNZIONE O DIMISSIONE DI UN SOGGETTO
- ATTIVAZIONE DI UN PERIODO DEFINITO DI STAGE E TIROCINIO FORMATIVO

## 1.3. DESTINATARI

I destinatari della procedura sono:

- Responsabile del Servizio Risorse Umane – Gruppo Operativo Risorse Umane (GORU) -
- Tutti i Responsabili di funzione e/o i Capo Ufficio
- Responsabile Gruppo Operativo Informatica (GOI/CED)
- Amministratori di sistema

## 2. FASI DEL P R O CE S S O

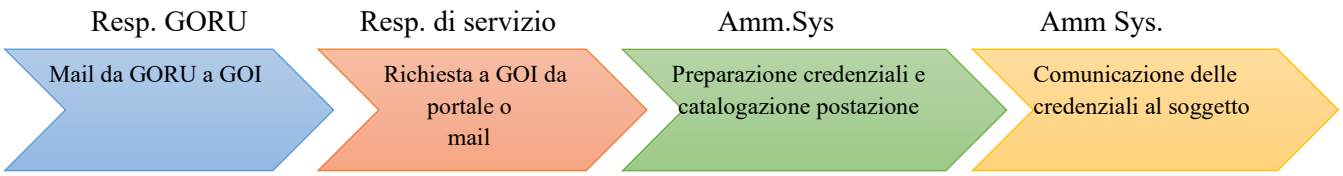
Il Responsabile del Gruppo Operativo Risorse Umane, di seguito GORU, dovrà inviare una comunicazione scritta tramite e-mail al Responsabile/Capo Ufficio del servizio che ospiterà il soggetto e al Responsabile del

Gruppo Operativo Informatica/CED, di seguito GOI, contenente le informazioni necessarie alla registrazione o de-registrazione del soggetto.

Il responsabile dell'ufficio/area in cui il soggetto prenderà servizio invierà una richiesta di supporto informatico per richiedere le credenziali di accesso per la postazione di lavoro tramite il portale di supporto informatico o tramite e-mail.

L'amministratore del Sistema informatico metterà in atto i criteri per la creazione delle credenziali di accesso del nuovo soggetto e gli incaricati del GOI posizioneranno la postazione di lavoro nei tempi concordati.

Le credenziali di accesso alla postazione di lavoro e tutte le informazioni necessarie per l'utilizzo della stessa verranno comunicate al soggetto con apposita procedura.



## 3. RUOLI, RESPONSABILITA' E MODALITA' OPERATIVE

Il Responsabile del GORU dovrà comunicare al Responsabile del Goi tramite e-mail le seguenti informazioni:

- NOME E COGNOME DEL SOGGETTO
- RUOLO DEL SOGGETTO
- DATA DI ASSUNZIONE/INIZIO TIROCINIO O STAGE
- UFFICIO/AREA DI ARRIVO (E PARTENZA IN CASO DI CAMBIO MANSIONE)
- DATA DI DIMISSIONE/FINE TIROCINIO O STAGE

Il Responsabile dell'ufficio/Area in cui prenderà servizio il soggetto dovrà effettuare una richiesta tramite il portale di supporto informatico per:

- RICHIEDERE LA POSTAZIONE DI LAVORO (FISSA O PORTATILE)
- RICHIEDERE LE CREDENZIALI DI ACCESSO ALLA POSTAZIONE DI LAVORO

L'amministratore del sistema informatico dovrà attivare le credenziali di autenticazione per accedere alla postazione di lavoro creando il profilo di dominio:

a) CREAZIONE DELLO USER E DELLA PASSWORD UNIVOCI
b) CREAZIONE DEL PROFILO DI DOMINIO
c) ASSOCIAZIONE DEL PROFILO AL GRUPPO DI DOMINIO

L'amministratore di Sistema o il Responsabile degli Asset, se nominato, procederà ad inventariare la postazione di lavoro con le informazioni che ne determinano l'associazione della stessa al soggetto alla quale è affidata.

- CATALOGAZIONE DELLA POSTAZIONE DI LAVORO NEL SISTEMA IT DI ASSET MANAGEMENT

L'Amministratore di Sistema comunicheranno le credenziali di accesso alla postazione di lavoro al soggetto al quale è affidata.

La revisione degli accessi e dei permessi avrà cadenza annuale. La disabilitazione delle utenze non più attive ma non comunicate dagli uffici competenti avverrà in maniera automatica.

## 4. RISCHI E MISURE DI SICUREZZA

| RISCHIO | MISURE DI SICUREZZA |
|---|---|
| Uso non autorizzato di credenziali altrui | Le credenziali verranno associate all'asset hardware |
| Password associata al nome utente debole | Attivazione "complessità password obbligatoria" con scadenza 90/120 giorni |
| Utilizzo delle credenziali per usi non consentiti | Controlli e verifiche periodiche |
| Utilizzo delle credenziali per attivazioni utenze non lavorative (password uguali per l'utente Social, per es.) | Regolamenti e sensibilizzazione |

## 5. RIFERIMENTI NORMATIVI, REGOLAMENTI, REVISIONE E ALLEGATI

Regolamento interno per l'utilizzo delle postazioni informatiche, della posta elettronica e di Internet par.3 e 4

- Regolamento interno per l'utilizzo delle postazioni informatiche, della posta elettronica e di Internet – par. 4 (All. 1)
- D.Lgs. 196/03 e s.m.i.
- Reg. EU 2016/679 e s.m.i.
- CAD – Codice dell'Amministrazione Digitale –

## 6. REVISIONI

| Data | Revisione | Creata da | Descrizione della modifica |
|---|---|---|---|
| 30/01/2023 | 0.2 | Resp.GOI | Aggiornamento responsabilità |
| | | | |

## 7. ALLEGATI

- Regolamento interno per l'utilizzo delle postazioni informatiche, della posta elettronica e di Internet (All. 1)

# PROCEDURA PER IL PROVISIONING DEGLI ACCESSI ALLE APPLICAZIONI

## 1 SCOPO, AMBITO DI APPLICAZIONE E DESTINATARI

### 1.1 Scopo

Lo scopo del documento è quello di illustrare, con una procedura chiara e condivisa, quali sono le operazioni, le responsabilità e i ruoli per richiedere ed ottenere le credenziali di autenticazione per l'utilizzo delle applicazioni aziendali e dei dati in esse contenuti. Il fine è quello di evitare che vi siano accessi non autorizzati che possano compromettere il funzionamento dell'applicazione, la perdita o la distruzione dei dati e delle informazioni.

### 1.2 Ambito di applicazione

La procedura si applica nei seguenti casi

- Richiesta di credenziali per l'accesso al Sistema IBM AS400
- Richiesta di credenziali per l'accesso al Sistema Documentale WEBRAINBOW
- Richiesta di credenziali per l'accesso al Sistema Contabile E-Solver
- Richiesta credenziali per applicativi verticali o "minori"

### 1.3. Destinatari

I destinatari della procedura sono: tutti gli amministratori di Sistema, il Responsabile del GOI e tutti i Capo Ufficio/Responsabili.

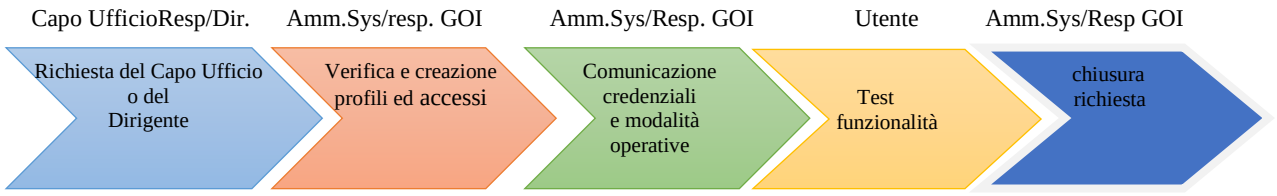
## 2 DESCRIZIONE DEL PROCESSO

Il processo ha inizio con la richiesta effettuata tramite comunicazione mail da parte del Capo Ufficio/Responsabile di settore o del Dirigente competente. Successivamente l'Amministratore di Sistema o il responsabile del GOI procederanno con la creazione degli accessi. L'utilizzatore dovrà accertarsi che il profilo creato sia completo di tutte le funzionalità necessarie per svolgere la propria attività e, nel caso ci fossero delle modifiche da effettuare, il Capo Ufficio/Responsabile di settore o il

Dirigente dovrà darne comunicazione tramite mail inviata al GOI e l'amministratore del sistema provvederà ad effettuare le variazioni richieste.

La procedura si potrà ritenere conclusa dopo la chiusura della richiesta da parte del Capo Ufficio/Responsabile di settore o del Dirigente competente tramite comunicazione mail.

La revisione degli accessi e dei profili avrà cadenza semestrale o annuale e, nel caso in cui vi sia l'evidenza che i dati dell'utenza (Password) abbiano perso la loro segretezza, verrà richiesto di modificare la password di accesso ai Sistemi e al Dominio "ESTSESIA" (accesso alla rete e alla postazione di lavoro).




## 3 RUOLI, RESPONSABILITA' E MODALITA' OPERATIVE

1) ***Il Capo Ufficio/Responsabile*** o il ***Dirigente del Servizio*** dovrà creare la richiesta di accesso tramite il modulo "Richiesta credenziali di accesso ai Sistemi". Le informazioni che dovranno essere specificate obbligatorie sono:

- Nome e cognome dell'utilizzatore
- Data Inizio e data fine (in caso di accesso temporaneo)
- Sede di appartenenza
- Servizio di appartenenza
- Ruolo
- Applicativi per i quali si richiede l'accesso e profilo di accesso

2) L'**Amministratore di Sistema** o il **Responsabile del GOI** dovrà effettuare una verifica delle informazioni per poi procedere con la creazione dei profili e delle credenziali di accesso

3) L'**Amministratore di Sistema** o il **Responsabile del GOI** comunicheranno all'utilizzatore le credenziali, con password temporanea, create per ogni applicativo abilitato e le modalità operative

4) L'**utente utilizzatore** dovrà obbligatoriamente, dopo il primo accesso, cambiare la password temporanea

5) L'utente utilizzatore comunicherà il buon funzionamento del profilo di accesso al **Capo Ufficio/Responsabile o al Dirigente del Servizio**.

5.a) In caso di modifiche al profilo la procedura riprenderà dal punto 2 dopo eventuali indicazioni del responsabile del servizio comunicate tramite mail

## 4 RISCHI E MISURE DI SICUREZZA

| RISCHIO | MISURE DI SICUREZZA |
|---|---|
| Uso non autorizzato di credenziali altrui | sensibilizzazione e gestione dei permessi tramite la suddivisione delle utenze in gruppi associati all'attività |
| Password associata al nome utente debole | Attivazione "complessità password obbligatoria" con scadenza 90 giorni per gli applicativi che hanno una policie automatica. |
| | |
| | |

## 5 RIFERIMENTI NORMATIVI, REGOLAMENTI, REVISIONE E ALLEGATI

- Regolamento interno per l'utilizzo delle postazioni informatiche, della posta elettronica e di Internet – par. 4 (All. 1)
- D.Lgs. 196/03 e s.m.i.
- Reg. EU 2016/679 e s.m.i.
- CAD – Codice dell'amministrazione Digitale -

**REVISIONI**

| Data | Revisione | Creata da | Descrizione della modifica |
|---|---|---|---|
| 30/03/2021 | 0.1 | Resp.IT | Aggiornamento modalità |
| | | | |

# “PROCEDURA PER L’ASSEGNAZIONE DEGLI ASSET TECNOLOGICI”

**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

Sommario

# 1. SCOPO, AMBITO DI APPLICAZIONE E DESTINATARI

## 1.1. Scopo

Lo scopo del presente documento è quello di illustrare il processo di assegnazione di un dispositivo hardware all'operatore al quale verrà associato.

Il fine è quello di regolamentare con un processo chiaro e condiviso le operazioni, le responsabilità e i ruoli di tutti gli attori coinvolti nel processo di assegnazione delle postazioni informatiche, dei dispositivi mobili e delle memorie di massa esterne, così da garantire che non vi siano asset tecnologici non autorizzati e non tracciati per tutto il loro ciclo vita.

## 1.2. Ambito di applicazione

La procedura si applica nei seguenti casi:

- RICHIESTA DI UNA NUOVA POSTAZIONE DI LAVORO
- CAMBIO DI MANSIONE E CAMBIO CONTESTUALE DELL'ASSET ASSEGNATO

## 1.3. Destinatari

I destinatari della procedura sono:

- Tutti i richiedenti (Capi Ufficio, Responsabili, Dirigenti)
- Utente utilizzatore dell'asset
- Responsabile GOI/CED
- Addetto PDL (postazioni di lavoro)

## 2. FASI DEL PROCESSO

Il Responsabile del Servizio in cui l'utente utilizzatore svolge le sue mansioni dovrà inviare il modulo "richiesta di assegnazione Asset" all'Amministratore di sistema, contenente le informazioni richieste e specificate sul modulo.

Il Responsabile del GOI/CED verificherà la richiesta e, se potrà essere accettata, incaricherà un addetto del GOI per la preparazione di quanto autorizzato. La richiesta potrebbe essere per più asset (es. dispositivo mobile e/o tablet e postazione di lavoro).

All'utilizzatore verrà fatto firmare il modulo di assegnazione asset per avere l'assegnazione tracciata e per responsabilizzare l'utilizzatore sul corretto utilizzo dell'Asset tecnologico e sulla sua custodia.


## *3. RUOLI, RESPONSABILITA' E MODALITA' OPERATIVE*

Il Richiedente dovrà inviare il "modulo di richiesta e assegnazione asset" al Responsabile GOI/CED, il modulo conterrà le seguenti informazioni:

- NOME E COGNOME DEL SOGGETTO
- UFFICIO
- SEDE DI LAVORO

L'amministratore del sistema informatico dovrà attivare le credenziali di autenticazione per

accedere alla postazione di lavoro creando il profilo di dominio:

a) CREAZIONE DELLO USER E DELLA PASSWORD UNIVOCI

b) CREAZIONE DEL PROFILO DI DOMINIO

c) ASSOCIAZIONE DEL PROFILO AL GRUPPO DI DOMINIO

L'amministratore di Sistema procederà ad inventariare la postazione di lavoro con le informazioni che ne determinano l'associazione della stessa al soggetto alla quale è affidata.

- CATALOGAZIONE DELLA POSTAZIONE DI LAVORO NEL SISTEMA INFORMATICO DI ASSET MANAGEMENT

Un addetto del GOI comunicherà le credenziali di accesso alla postazione di lavoro al soggetto al quale è affidata.

La revisione degli accessi e dei permessi avrà cadenza annuale. La disabilitazione delle utenze non più attive ma non comunicate dagli uffici competenti avverrà in maniera automatica.

## *4. RISCHI E MISURE DI SICUREZZA*

| RISCHIO | MISURE DI SICUREZZA |
|---|---|
| Utilizzo di asset non autorizzati | Con la catalogazione degli asset autorizzati e censiti si ha la possiblità di effettuare una revisione periodica delle autorizzazioni e dell'associazione HW → utente autorizzato |
| Utilizzo di memorie di massa esterne non autorizzate | |
| Perdita della tracciabilità e del controllo del ciclo vita dell'asset | L'associazione utente/apparato consente di controllare se ci sono soggetti che utilizzano asset non a loro assegnati |
| Appropriazione indebita di asset aziendali | |

## 5. *RIFERIMENTI NORMATIVI, REGOLAMENTI, REVISIONE E ALLEGATI*

- Regolamento interno per l'utilizzo delle postazioni informatiche, della posta elettronica e di Internet (All. 1)

6. D.Lgs. 196/03 e s.m.i.
7. Reg. EU 2016/679 e s.m.i.
8. CAD – Codice dell'amministrazione Digitale -

## *6. REVISIONI*

| Data | Revisione | Creata da | Verificata da | Aurorizzata da |
|---|---|---|---|---|
| 01/02/2021 | 0.1 | Dott. Gianluca Manzini | Avv. Elena Nale<br><br>Dott. Roberto Occhipinti | Direttore generale |
| | | | | |

## *7. ALLEGATI*

- Modulo di richiesta e assegnazione asset tecnologico (All. 2)

# Regolamento interno
# per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet

| Rev. | Data | Redatto | Verificato | Approvato |
|---|---|---|---|---|
| 02.2021 | 11/09/2021 | Dott. Gianluca Manzini | Avv.Elena Nale<br>Dott. Roberto Occhipinti | Direttore Generale |

**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

# Sommario





**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

**PREMESSA**

Le realtà aziendali si caratterizzano per l'elevato uso della tecnologia informatica che, da un lato, ha consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda al dipendente per lo svolgimento delle proprie mansioni.

Il momento storico sta dando, inoltre, una accelerazione all'utilizzo di apparati digitali interconnessi tra loro e, anche per questo motivo, é fortemente sentita dalla Direzione del Consorzio Est Sesia la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti, cercando di impedire conseguentemente, gli usi scorretti che, oltre ad esporre l'azienda stessa a rischi tanto patrimoniali quanto penali, sono contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile.

I controlli preventivi sull'uso di apparati informatici devono garantire il diritto del datore di lavoro a proteggere la propria organizzazione, essendo tali apparati strumenti di lavoro la cui utilizzazione personale è preclusa. Deve essere inoltre garantito il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi, il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dalla normativa vigente in materia di protezione dei dati personali (Reg. UE 679/2016, Dlgs. 196/2003 così come modificato dal D.Lgs. 101/2018 e s.m.i.).

Il Consorzio Est Sesia, per quanto già esplicitato, ha avviato un percorso di aggiornamento e di rafforzamento delle proprie politiche di sicurezza informatica, al fine di garantire l'integrità e la disponibilità dei dati trattati, tenendo conto delle specifiche normative e prescrizioni nazionali ed internazionali dettate in materia.

È dovere del Consorzio Est Sesia individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità.

L'utilizzo delle apparecchiature informatiche (ed in particolare l'accesso alla rete informatica, Internet e posta elettronica, dalla propria sede o da remoto) e la messa a disposizione da parte del Consorzio al proprio personale di telefoni e strumenti informatici (computer fissi e portatili, tablets, telefoni cellulari, smartphone, etc.) come strumenti di lavoro, impone la necessità di regolamentarne l'utilizzo, attraverso specifiche disposizioni.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

Il Regolamento ha lo scopo di fornire agli utenti un'adeguata informazione circa i doveri e le conseguenti modalità che ciascuno deve osservare per il corretto uso di detta strumentazione, nello svolgimento del proprio lavoro presso gli uffici delle sedi ed anche in modalità "agile" (Smart-Working), in modo da consolidare ancora maggiormente le politiche di sicurezza messe in atto.

Vige in capo al personale che svolge a qualsiasi titolo attività lavorativa nella struttura del Consorzio l'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli a beni mobili ed agli strumenti ad essi affidati. Vige altresì l'obbligo di non utilizzare a fini privati informazioni, documenti, filmati, foto o attrezzature di cui dispone per scopi lavorativi.

Ogni utente è responsabile disciplinarmente, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali ed è altresì responsabile del contenuto delle comunicazioni effettuate e ricevute anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.

Sono altresì vietati comportamenti che possano creare un danno, anche di immagine, al Consorzio Est Sesia e/o ai suoi dipendenti ed Amministratori (commenti sui Social Network, utilizzo non consentito di informazioni lavorative soprattutto se riservate, per esempio).

Il Regolamento ha la funzione di disciplinare la materia individuando criteri e modalità operative di accesso ed utilizzo dei dispositivi informatici, della rete di computer, di Internet e della posta elettronica del Consorzio Est Sesia da parte dei dipendenti e di tutti gli altri soggetti che, a vario titolo, prestano servizio o attività per conto e nelle strutture dell'Ente (a titolo esemplificativo: collaboratori, liberi professionisti, ecc.), oltre che da parte di utenti esterni (persone fisiche, aziende private e pubbliche e ditte fornitrici) che, sulla base di rapporti contrattuali o convenzionali, autorizzati dalla Direzione del Consorzio, accedono dall'esterno utilizzando alcune componenti del Sistema Informativo aziendale.

Lo schema di Regolamento di seguito riportato viene incontro alle esigenze menzionate, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e per informare adeguatament gli stessi e ai sensi dell'art. 13 del Reg. UE 679/2016 (di seguito GDPR) e agli obblighi in merito alle misure di sicurezza disciplinate dall'art. 32 del GDPR.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

## 1. ENTRATA IN VIGORE DEL REGOLAMENTO.

1.1. Il nuovo regolamento entrerà in vigore il **12/10/2021.**

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Verrà, inoltre, inviata tramite mail comunicazione a ciascun utente dell'avvenuta pubblicazione del Regolamento sul Sistema Informativo Documentale "Webrainbow" tramite Circolare. Lo stesso Regolamento sarà poi inserito anche in "Vdati". Verrà distribuita una copia cartacea in ogni Ufficio della sede di Novara e delle sedi/Distretti Esterni, nonchè affissa in luoghi accessibili a tutti.

Verranno organizzate sessioni di informazione sulle norme contenute nel presente Regolamento.

Le modalità di diffusione del presente regolamento sono compatibili con quanto previsto dall'art.7 dello Statuto dei lavoratori.

## 2. CAMPO DI APPLICAZIONE DEL REGOLAMENTO.

2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Consorzio a prescindere dal rapporto contrattuale con la stessa intrattenuto (dipendenti, consulenti, collaboratori, ecc).

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche, per "utente" deve intendersi ogni persona fisica (come già sopra citato, a titolo esplicativo: dipendenti, consulenti, fornitori di servizi, collaboratori, ecc) in possesso di specifiche credenziali di autenticazione informatica – nome utente e password.

## 3. UTILIZZO DELLA POSTAZIONE DI LAVORO – PERSONAL COMPUTER.

3.1 Il personal computer (PC) affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere preservato con cura evitando ogni possibile forma di danneggiamento.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

3.2 Il personal computer affidato all'utente permette l'accesso alla rete del "Consorzio di irrigazione e bonifica EST SESIA", di seguito per brevità "Consorzio", solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 Il Consorzio rende noto che il personale incaricato che opera presso il Gruppo Operativo Informatica del Consorzio, di seguito per brevità "GOI", è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del Sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi necessari e/o richiesti (aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware ecc.).
Detti interventi, in considerazione dei divieti di cui ai successivi punti nr. 8.2 e 9.2, potranno anche comportare l'accesso ai file di log del Sistema Operativo e del browser Internet del PC dell'utente, l'accesso ai dati trattati dall'utente e al software di gestione della posta elettronica dell'utente. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Consorzio, si applica anche in caso di assenza prolungata o impedimento dell'utente.

3.4 Il personale incaricato del GOI ha la facoltà di svolgere le attività sulle postazioni informatiche anche da remoto, previa autorizzazione verbale dell'utente o del responsabile, al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento sarà effettuato utilizzando i software di controllo remoto "VNC", "Microsoft Windows Remote Desktop" e "Team Viewer". Durante l'intervento da remoto tutte le attività, svolte non in presenza, saranno comunque sempre visibili e controllabili dall'utente.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del GOI per conto del Consorzio, né viene consentito agli utenti di installare autonomamente programmi software di qualunque genere, sussistendo il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone il Consorzio a gravi responsabilità; si evidenzia che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di applicativi regolarmente licenziati, espone il Consorzio a gravi sanzioni amministrative e penali[1].

[1] Artt. 171-ter e 174-ter del D.Lgs. 248/2000 e s.m.i. cp



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

3.6 Salvo preventiva, espressa autorizzazione del personale del GOI, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio dispositivi per la connessione Internet, dispositivi USB, Hard Disk esterni, ecc).

3.7 Ogni utente deve prestare la massima attenzione ai supporti "autorizzati" di origine esterna menzionati al precedente punto 3.6, avvertendo immediatamente il personale del GOI nel caso in cui rilevasse anomalie - avvisi del software antivirus o situazioni riconducibili ad una infezione da virus informatico - ed adottando quanto previsto dal successivo punto 10.2 del presente Regolamento relativo alle "istruzioni operative in caso di infezione informatica".

3.8 Il Personal Computer e il monitor devono essere spenti ogni sera prima di lasciare gli uffici, salvo i casi in cui un utente debba collegarsi da casa tramite il software Guacamole. In ogni caso devono essere messi in "blocco" prima di lasciare la postazione premendo contemporaneamente "ctrl/alt/canc + invio o barra spaziatrice", in caso di assenze prolungate dall'ufficio o in caso di inutilizzo prolungato.
Anche se la gestione delle connessioni da remoto è controllata e sicura durante l'utilizzo dei software, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso indebito (il blocco del pc tramite i comandi sopra citati è indispensabile, così come la gestione corretta delle proprie password, così come specificato al seguente punto 4).

## 4. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE.

4.1 Le credenziali di autenticazione dell'utente, composte da "nome utente" (user) e "parola chiave" (di seguito denominata "password"), vengono assegnate dal personale del GOI previa richiesta del Capo ufficio/Responsabile del settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
La stessa modalità si applica anche per i soggetti esterni e temporanei come i consulenti, i collaboratori e i fornitori di servizi; le credenziali saranno attive per il tempo necessario ad espletare le attività a loro assegnate (in questi casi le credenziali saranno configurate con scadenza temporale, da "n" ore a "n" giorni/mesi).



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

4.2 La password è riservata e potrà essere cambiata dall'utente in qualsiasi momento; dovrà essere conservata con la massima diligenza e mai divulgata a terzi o a persone non autorizzate (non deve essere esposta, resa visibile o essere identificabile).

4.3 La parola chiave deve rispettare uno o più "criteri di complessità" con le seguenti caratteristiche:

- Lunghezza minima 8 caratteri
- Caratteri maiuscoli dell'alfabeto inglese (A-Z)
- Caratteri minuscoli dell'alfabeto inglese (a-z)
- Cifre decimali (0-9)
- Caratteri non alfabetici, ad esempio !, $, #, %

Esempio: Tulipano!2002 oppure _Tulipano2002 oppure Tulipano!2002$ oppure tuliP@no2002

4.4 Il Sistema sarà configurato entro la fine dell'anno per fare in modo che l'utente sia obbligato a modificare la password creata dal GOI al primo accesso.

4.5 Qualora la parola chiave (password) dovesse essere sostituita, per decorso del termine previsto (3 o 6 mesi) e/o in caso di perdita della sua riservatezza, l'utente procederà al cambio password in autonomia (il server di dominio avvisa che la password sta per scadere e propone il cambio) o con il supporto del GOI, se necessario.

4.6 Al fine di raggruppare le tipologie di dati ai quali gli incaricati possono accedere e al fine di identificare i trattamenti che sono necessari per lo svolgimento delle loro mansioni lavorative, sono in uso opportune misure tecniche di autorizzazione. Le autorizzazioni all'accesso sono generalmente impostate per classi omogenee di incaricati e vengono rilasciate e revocate dal GOI su richiesta, in caso di cambio mansion di uno o più soggetti e in caso di riorganizzazione. Tali profili autorizzativi vengono definiti con l'obiettivo di limitare l'accesso ai dati che sono indispensabili per svolgere le proprie mansioni lavorative.

4.7 È opportuno che il GOI proceda con cadenza almeno annuale ad un controllo effettivo di consistenza delle utenze attive (sia con riferimento alle utenze interne, che a quelle esterne), al fine di verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

Tale review delle utenze deve essere formalizzata e tracciata, e prevede la disattivazione di quegli utenti che non effettuano l'accesso da più di sei mesi, se non vengono individuate specifiche esigenze per il loro mantenimento.

## 5. UTILIZZO DELLA RETE DEL CONSORZIO EST SESIA.

5.1 Il Sistema Informativo di EST SESIA è strutturato nel cosiddetto "dominio locale", denominato "AIES", cui ogni personal computer è connesso per mezzo della rete locale e MPLS. Le regole governate dal dominio (policies) garantiscono la sicurezza della rete informativa aziendale e la condivisione delle informazioni. Ogni apparecchiatura informatica e l'utente che ne fa uso, sono soggetti a tali regole e solo eventuali difficoltà tecnico-operative, o esigenze temporanee, valutate dal Responsabile del Gruppo Operativo Informatica, possono consentirne la deroga.
Per accedere alle risorse della rete aziendale, ciascun utente deve essere in possesso delle specifiche credenziali come specificato al precedente punto 4.1.

5.2 È assolutamente proibito utilizzare codici identificativi di altri utenti.

5.3 Le banche dati (cartelle e repository) presenti nei file server, nelle NAS (dischi esterni autorizzati) e nel Sistema Documentale del Consorzio sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, i file non utilizzati per le attività lavorative (file personali) non possono essere dislocati, nemmeno per brevi periodi, in queste unità.
Si ricorda che né i dischi né altre unità di memorizzazione locali (es. disco C: del PC) sono soggetti a salvataggio da parte del personale incaricato del GOI. La responsabilità dell'eventuale perdita o della cancellazione dei dati ivi contenuti è, pertanto, a carico dell'utente.

5.4 Il personale del GOI può, dopo un primo avviso, procedere alla rimozione di file o applicazioni ritenute pericolose per la Sicurezza dei dati e delle applicazioni aziendali. La rimozione dei file può essere effettuata sia sui PC degli utenti che sulle unità di rete.

5.5 Risulta opportuno che ciascun utente provveda, se non ancora fatto, a spostare tutto il materiale legato all'attività lavorativa dagli archivi locali nelle cartelle di rete messe a disposizione.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

## 6. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI.

6.1 Tutti i supporti di memorizzazione rimovibili (Hard Disk esterni, supporti USB, ecc.), l'uso dei quali deve essere autorizzato dal personale del GOI, contenenti dati 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.

6.2 È vietato l'utilizzo di supporti rimovibili personali non autorizzati.

6.3 L'utente è sempre responsabile dei supporti a lui affidati e dei dati aziendali in essi contenuti[2].

## 7. UTILIZZO DI PC PORTATILI E DISPOSITIVI SMARTPHONE/TABLET.

7.1 L'utente è responsabile del pc portatile, del tablet, del cellulare e dello smartphone (in seguito denominati "dispositivi mobili") a lui assegnati. L'utente deve custodire i dispositivi mobili con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.

7.2 A tutti i dispositivi mobili si applicano i principi di utilizzo previsti dal presente regolamento, con particolare attenzione alla rimozione di eventuali file creati ed elaborati ma non salvati sulle cartelle dei server aziendali prima della riconsegna.

7.3 L'utilizzo dei dispositivi mobili è consentito solo per scopi lavorativi. L'utilizzo degli apparati da casa deve essere autorizzato dal Dirigente o dal Responsabile/Capo Ufficio.

7.4 L'utilizzo dei dispositivi mobili per un uso diverso da quello per il quale sono stati assegnati all'utente è passibile di richiamo o sanzione disciplinare.

7.5 Occorre prestare attenzione a non lasciare incustodito lo strumento in viaggio in caso di PC portatili (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici).

7.6 È vietato lasciare incustodito sull'autovettura lo strumento aziendale, anche se per soste brevi, indipendentemente dalla visibilità o meno dello strumento dall'esterno.

[2] "Procedura di assegnazione asset"



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

## 8. USO DELLA POSTA ELETTRONICA.

8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica aziendali - @estsesia.it, per es. - per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati/ brani musicali (es.mp4/mpeg/avi/streaming/ecc.) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la condivisione, tramite l'invio, di messaggi che chiedono denaro/aiuto o simili. Se si dovessero peraltro ricevere messaggi di tale tipo, lo si deve comunicare immediatamente al personale del GOI. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

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

8.4 È fatto divieto di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.

8.5 Tutte le cassette postali archiviano automaticamente la posta elettronica giornalmente su banche dati preposte alla loro conservazione.

8.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati al messaggio di posta elettronica. E' vietato salvare o aprire allegati contenenti file con estensioni non conosciute (per esempio file .exe/.bat/.vbs).



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

8.7 È assolutamente vietato cercare di aprire collegamenti link – indirizzi o parole, solitamente blu e con sottolineatura, che si possono selezionare ("cliccare") – inseriti nel corpo o nell'oggetto del messaggio di posta elettronica se non identificati come elementi sicuri e compatibili con l'attività lavorativa e con i sistemi utilizzati.

Sono da eliminare, informando il GOI, tutti i messaggi che arrivano da mittenti non conosciuti e i messaggi con contenuto "anomalo" legato e non alla propria attività lavorativa tra cui, a titolo di esempio:

- mail che vi informano che sono variate le coordinate bancarie di un fornitore o per il pagamento di fatture (chiamare la banca o il fornitore per avere un riscontro);
- mail in arrivo da gestori pubblici che informano che siete debitori (ENEL, ENI, gestori telefonici, società di credito, banche, autorità giudiziarie, ecc);

mail con caratteristiche particolari:

- mail il cui contenuto non risulti scritto in un italiano corretto [mail virus tradotte con sistemi informatici (google translator per es.)];
- mail che arrivano da indirizzi mail con dominio "anomalo" (@.....org, @....biz, @...., ecc);
- mail che contengono documenti che normalmente, durante lo svolgimento del vostro incarico, non vi vengono inviati;
- mail che contengono allegati in formato .xls o .doc e che dovrebbero essere inviate in formato .pdf (fatture, ordini, DDT, ecc.);
- mail con allegati in formato compresso - .zip/.rar – se non concordati direttamente con il mittente.

8.8 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, in caso di assenze programmate (es. per ferie o per malattia prolungata), il sistema dovrà essere configurato per inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre modalità per contattare EST SESIA (messaggio di avviso del "fuori sede").

L'assegnatario della casella (il "delegante") può, in alternativa, anche chiedere di configurare un inoltro dei messaggi ricevuti su un altro indirizzo mail, previa autorizzazione scritta del soggetto preposto (il "delegato").

Nel primo caso – fuori sede - l'assegnatario della casella mail dovrà procedere in autonomia; nel secondo caso – inoltro su altro indirizzo mail – l'assegnatario della casella mail si dovrà rivolgere al GOI.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

8.9 In caso di assenza non programmata (ad es. per malattia) e/o nei casi in cui non possa essere eseguita la procedura di attivazione del messaggio "fuori sede", la stessa potrà essere attivata a cura del GOI, previa autorizzazione dell'assegnatario della casella o del responsabile di funzione o del Dirigente del servizio.

8.10 È consentito incaricare un delegato e dare le istruzioni per poter accedere alla casella di posta elettronica nei casi in cui si renda necessario e su richiesta del Responsabile di funzione o della Direzione (per la gestione dei messaggi della casella di posta elettronica assegnata o per lo smistamento verso il protocollo, per esempio).

## 9. NAVIGAZIONE INTERNET.

9.1 Il PC/mobile assegnato all'utente è abilitato alla navigazione in Internet. La navigazione può essere effettuata esclusivamente per lo svolgimento della propria attività lavorativa.

In questo senso, a titolo puramente esemplificativo, il PC/mobile non deve utilizzare Internet per:

- l'upload o il download di software gratuiti, in prova o a pagamento, nonché di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa previa verifica dell'attendibilità dei siti in questione. E' assolutamente vietato il download di allegati in formato .bat/.exe/.vbs/.sql./mdb onon conosciuti (i documenti, inoltre, dovrebbero essere in formato .pdf e non in formati office - .xls/.doc/.ppt/);
- l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione;
- ogni forma di registrazione e di accesso a siti i cui contenuti non siano strettamente legati all'attività lavorativa (Social network come Facebook, Twitter, Instagram, Linkedin; siti di interesse personale, siti di E-Commerce, ecc.), fatti salvi i casi direttamente autorizzati dalla Direzione;
- la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

9.2 EST SESIA rende peraltro nota, al fine di evitare la navigazione in siti non pertinenti e non sicuri, l'adozione di uno specifico sistema di blocco, o filtro automatico, che prevenga determinate operazioni quali, per esempio, l'upload o l'accesso a siti internet inseriti in una black list.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

Gli eventuali controlli, compiuti dal personale incaricato del GOI ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di verifica dei contenuti o mediante analisi dei "file di log" della navigazione Internet in maniera anonima, nel completo rispetto della privacy.

## 10. PROTEZIONE ANTIVIRUS.

10.1 Il sistema informatico di EST SESIA è protetto da un software antivirus che si aggiorna quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di "infezione informatica" causata da virus, malware, spyware e simili.

10.2 Istruzioni operative in caso di "infezione informatica".

Nel caso in cui il software antivirus rilevi la presenza di un'infezione o nel caso in cui sia l'utente stesso ad accorgersi che vi sia una minaccia in corso, le operazioni da effettuare sono:

1. interrompere ogni elaborazione senza chiudere eventuali file aperti;
2. segnalare immediatamente l'accaduto al personale del GOI.

## 11. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.

11.1 È obbligatorio attenersi alle disposizioni in materia di Privacy come indicato nella lettera di designazione ad autorizzato al trattamento dei dati ai sensi dell'art. 32 del Reg UE 2016/679 e del D.Lgs. n. 196/2003 così come modificato dal D.Lgs 101/2018.

## 12. ACCESSO AI DATI TRATTATI DALL'UTENTE.

12.1 È facoltà della Direzione del Consorzio, tramite il personale del GOI, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti. Oltre che per motivi di sicurezza del sistema informatico, tale accesso diretto potrà avvenire anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, dell'hardware, etc.) e per una corretta gestione dei costi previsionali (sostituzione degli apparati o dei sistemi applicativi installati).



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

Si fa presente che il personale del GOI è stato nominato "Amministratore di Sistema", così come previsto dal GDPR.

## 13. SISTEMI DI CONTROLLO GRADUALI.

13.1 In caso di anomalie (uso indebito della linea Internet, chat non autorizzate, ripetuti tentativi di accesso a cartelle di rete senza autorizzazione, ecc.), il personale del GOI effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia. Si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente alle istruzioni impartite nel presente regolamento. In caso di successive ulteriori anomalie riscontrate nella stessa area o settore verranno compiuti controlli più circoscritti per individuare la fonte dell'anomalia.

13.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## 14. LAVORO AGILE – SMART-WORKING.

14.1 Quanto di seguito regolamentato annulla e sostituisce integralmente la dispozione n. 10 del 12/07/2019.

14.2 La creazione di un collegamento VPN a favore di un Dipendente deve essere motivata e autorizzata dal Direttore Generale, specificandone la durata, e operata dal CED.

14.3 Apposita registrazione sarà predisposta dal CED e conservata presso il GORU che annoterà su scadenziario la suddetta durata; il CED darà apposita documentazione al GORU dei collegamenti in atto alla data della presente disposizione.

14.4 Il GORU informerà il CED dell'andata in quiescenza dei Dipendenti o delle interruzioni dei rapporti di lavoro affinché si provveda tempestivamente alla disattivazione dei vari profili e di eventuale collegamento VPN.



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

14.5 Gli strumenti informatici messi a disposizione del lavoratore agile (ad esempio, computer portatile, accessori, software, ecc.) sono di proprietà del Consorzio Est Sesia che rende disponibile sulla postazione di lavoro virtuale gli strumenti software necessari per l'utilizzo dei servizi applicativi in un contesto di sicurezza e omogeneizzazione delle stesse postazioni di lavoro.

14.6 Il lavoratore deve utilizzare le applicazioni, Internet, la posta elettronica e i servizi informatici in modo appropriato e diligente anche se utilizza il proprio computer personale. Si ricorda che dal prorpio pc personale, durante il lavoro in modalità "agile", si accede in ogni caso ai Sistemi Informativi del Consorzio Est Sesia.
La posta elettronica e Webrainbow, per esempio, sono consultabili tramite Internet ma gli applicativi risiedono sugli apparati server del Consorzio.

14.7 Per l'utilizzo dei servizi da remoto (da casa/fuori sede) il Dipendente accede mediante il Sistema VPN SSL (Virtual Private Network) messo a disposizione del CSI Piemonte o mediante il software di collegamento remoto Guacamole, di proprietà del Consorzio Est Sesia.

14.8 Sono assolutamente vietati ulteriori Sistemi di collegamento se non autorizzati dal Personale del GOI.

## 15. AGGIORNAMENTO, REVISIONE E LEGGI DI RIFERIMENTO

15.1 Il Regolamento è soggetto ad aggiornamento periodico.

15.2 Leggi di riferimento.

**NORMATIVA EUROPEA**

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati personali").



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

**NORMATIVA ITALIANA**

- Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni ("Codice in materia di protezione dei dati personali").
- Legge 20 maggio 1970, n. 300, norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento (detta anche "statuto dei lavoratori").
- Decreto Legislativo 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Azienda e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.
- Codice Civile:
  - Art. 2049: Responsabilità indiretta dell'imprenditore;
  - Art. 2086: Direzione e gerarchia nell'impresa;
  - Art. 2087: Tutela dell'integrità fisica e della personalità morale dei dipendenti, da parte dell'imprenditore;
  - Art. 2104: Diligenza del dipendente nel rispetto delle disposizioni impartite dall'imprenditore.

**PROVVEDIMENTI AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

- Linee Guida del Garante Privacy su Posta Elettronica e Internet (Deliberazione n. 13 del 1° marzo 2007 – G.U. n. 58 del 10 marzo 2007).
- Provvedimento del Garante Privacy del 27 novembre 2008 e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema".



**Associazione Irrigazione Est Sesia**

**Sede centrale**
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152

Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

est sesia
consorzio di irrigazione e bonifica

# MODULO DI ASSEGNAZIONE ASSET TECNOLOGICO

## DATI DELL'ASSEGNATARIO

| | |
|---|---|
| **NOME** | |
| **COGNOME** | |
| **UFFICIO** | |
| **SEDE DI LAVORO** | |

## DATI DELL'ASSET TECNOLOGICO ASSEGNATO

| | |
|---|---|
| **TIPOLOGIA** | |
| **MARCA** | |
| **MODELLO** | |
| **S.N.** | |
| **DATA DI ASSEGNAZIONE** | |

**Associazione Irrigazione Est Sesia**
Sede centrale
via Negroni, 7
28100 Novara NO
Tel. +39 0321 675 211
Fax +39 0321 398 458
Casella postale nr. 152
Codice Fiscale 80000210031
Partita IVA 00533360038
e-mail: info@estsesia.it
pec: estsesia.pec@legalmail.it
www.estsesia.it

# NORME PER L'UTILIZZO DEL PERSONAL COMPUTER AZIENDALE

Il personal computer (fisso o portatile) affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere preservato con cura evitando ogni possibile forma di danneggiamento.

L'Associazione di irrigazione e bonifica Est Sesia Novara, di seguito EST SESIA Novara, rende noto che il personale incaricato che opera presso il "Gruppo Operativo Informatica", di seguito GOI, di EST SESIA Novara è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware ecc.). Detti interventi potranno anche comportare l'accesso ai file di log del Sistema Operativo e del browser Internet del PC dell'utente, l'accesso ai dati trattati dall'utente e al software di gestione della posta elettronica dell'utente. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente.

Il personale incaricato del GOI ha la facoltà di svolgere le attività sulle postazioni informatiche anche da remoto, previa autorizzazione verbale o scritta dell'utente o del responsabile, al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, ecc. L'intervento sarà effettuato utilizzando i software di controllo remoto "VNC", "Windows Desktop Remoto" e "Team Viewer". Durante l'intervento da remoto tutte le attività, svolte non in presenza, saranno comunque sempre visibili e controllabili dall'utente.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del GOI per conto di EST SESIA Novara né viene consentito agli utenti di installare autonomamente programmi software di qualunque genere, sussistendo il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L’inosservanza della presente disposizione espone la stessa Associazione di irrigazione e bonifica Est Sesia Novara a gravi responsabilità; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d’autore sul software, che impone la presenza nel sistema di applicativi regolarmente licenziati, espone, soprattutto, a gravi sanzioni amministrative.

Salvo preventiva, espressa autorizzazione del personale del GOI, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio dispositivi per la connessione Internet, dispositivi USB, Hard Disk esterni, ecc).

Ogni utente deve prestare la massima attenzione ai supporti “autorizzati” di origine esterna avvertendo immediatamente il personale del GOI nel caso in cui rilevasse anomalie - avvisi del software antivirus o situazioni riconducibili ad una infezione da virus informatico.

Il Personal Computer e il monitor devono essere spenti ogni sera prima di lasciare gli uffici o messi in “blocco” in caso di assenze prolungate dall'ufficio e in caso di inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso indebito.

IL RICHIEDENTE

……..

L’ASSEGNATARIO
Per accettazione

……