APROBAT
Proces – Verbal nr. 38 din 26 septembrie 2022

Președinte al Comitetului de Conducere
Malcoci Veronica _____

Politica privind protecția datelor și securitatea informației:

Versiunea 2.2

Grazer Wechselseitige Versicherung AG

GRAWE CARAT Asigurări

Versiunea	Data	Modificarea	Autor	Aprobare	Data publicării
5.0	07.03.2013	Primul proiect	Stoc		
5.1	21/03/2013	Revizuire	GL, AL de IT		
5.2	16/04/2013	Revizuire	Stoc	Kreinz	05/2013
5.3	25.10.2013	Revizuire	Stoc		
5.4	11.11.2013	Revizuire	Thelesklav, Titz		
5.5	21/03/2014	Formatare	Vodica		
6	05-2016	Adaptare la ISO 27001	Stoc	Reiter	06/2015
6.1	10/2017	Pt. 6 Protecția datelor	Stoc	Reiter	10/2017
1.0	08/2018	Extensiile GDPR, redenumire	Stoc/Titz	Reiter	08/2018
2.0	08/2019	GDPR, clasificarea	Stoc/Titz	Reiter	08/2019
2.1	10/2020	Comunicațiile Video, capitolul. 10	Stoc/Titz	Spangl	10/2020
2.2	06/2021	Politica Pwd	Stoc / Titz	Spangl/Puhr	06/2021

Cuprins

1. General

1.1 SCOPUL

Domeniul de aplicare al acestei politici obligatorii de protecție a datelor și de securitate a informației (ulterior politică) acoperă întregul Grup GRAWE cu toate companiile afiliate, în măsura în care acestea utilizează infrastructura TI GRAWE.

Prezenta Politica a fost aprobată de Comitetul de Conducere al C.A ,,GRAWE CARAT Asigurări" S.A, și este **obligatorie pentru toți utilizatorii**. Fiecare utilizator este obligat să respecte politica prezentată aici, iar persoanele responsabile de executarea prezentei Politici trebuie să asigure conformitatea utilizării conform mijloacelor de care dispun.

Termeni cu caracter personal în cadrul acestei politici nu au nici o semnificație specifică de gen.

Această politică în versiunea sa actuală, este o parte integrantă a contractului de muncă. Ea poate fi schimbată, modificată sau revocată de GRAWE CARAT Asigurări în orice moment.

Dacă prevederile prezentei politicii de securitate a informației nu sunt respectate, atunci drepturile de utilizare a sub-zonelor infrastructurii TI GRAWE (acces la Internet etc.) pot fi restricționate pentru utilizator, blocate pentru o anumită perioadă de timp sau alternativ complet revocate.

În plus, angajații sunt atenționați , ca încălcările acestei politici ar putea duce la aplicarea sancțiunilor disciplinare.

1.2 IMPLEMENTAREA

Politica intră în vigoare la lansarea și distribuția sa în interiorul companiei și, prin urmare, înlocuiește documentele cu politici precedente.

1.3 RESPONSABILI

Companie	Pentru conținut	Pentru distributie	Aprobare
GRAWE AG	Manager de securitate TI	Manager de securitate TI	Directorul TI
GRAWE CARAT	Șef Departament TI	Șef Departament TI	Comitetul de Conducere

Tabelul 1: responsabilități

Persoanele responsabile de executarea prezentei Politici sunt încurajate să acționeze ca exemplu în domeniul securității TI, să explice angajaților conținutul politicii securității datelor și informației dacă este necesar și să-și ghideze angajații în timpul muncii de zi cu zi.

1.4 DEFINIȚIA TERMENILOR

1.4.1 Departament TI Group

Departamentul de servicii TI al Grazer Wechselseitige Versicherung AG situat în Graz, Pestalozzistraße, 73.

1.4.2 Departament TI local

Departamentul TI al GRAWE CARAT Asigurări, situat pe strada Alexandru cel Bun, 51, Chișinău.

1.4.3 Programe malware

Acest termen generic reprezintă, dar nu se limitează la un software dăunător, cum ar fi viruși de computer, viermi, cai troieni, ransomware, spyware, adware și scareware. Termenii „malware” și „viruși” sunt folosiți ca sinonimi.

1.4.4 Utilizator

Fiecare angajat care folosește un ID de utilizator personal pentru a obține acces la sistemele TI.

1.4.5 Numele de utilizator

Numele de utilizator și parola reprezintă împreună ID-ul utilizatorului. Numele de utilizator este partea statică; parola trebuie schimbată pentru toate sistemele la intervale regulate.

1.4.6 Infrastructura TI GRAWE

Toate sistemele și dispozitivele TI care sunt utilizate pentru prelucrarea electronică a datelor în companie. Acestea includ, dar nu se limitează la PC-uri, laptopuri, imprimante, dispozitive periferice (mouse, tastatură), smartphone-uri, servere, componente de rețea, cablare.

1.4.7 Rețeaua GRAWE

Conectarea în rețea a componentelor individuale ale infrastructurii TI GRAWE prin conexiuni de rețea. Un dispozitiv poate comunica cu alte componente de îndată ce este conectat la rețea.

1.4.8 Rețeaua client

Părți ale rețelei GRAWE, care sunt utilizate în mod exclusiv de către utilizatorii finali. De exemplu, rețelele Wi-Fi în birouri, acces la rețea în birouri.

1.4.9 SecMail

Soluție TI centrală pentru transportul de e-mail criptat către destinatari externi. Pentru detalii, consultați SharePoint (https://sharepoint.grawe.at/abteilungen/GD_IT/Seiten/GRAWE-Secure-eMail-Gateway.aspx).

1.4.10 Contract de prelucrare a datelor

Este obligatorie încheierea unui Contract de prelucrare a datelor cu orice furnizor sau contractant extern, dacă sunt prelucrate date cu caracter personal provenite de la GRAWE CARAT Asigurări.

1.4.11 Terț

Toate persoanele care nu sunt obligate să respecte această politică.

1.4.12 Procesarea datelor

Prelucrarea datelor cu caracter personal înseamnă orice proces efectuat, cu sau fără ajutorul unor proceduri automate, cum ar fi colectarea, organizarea, stocarea, adaptarea sau modificarea, citirea, interogarea, utilizarea, dezvăluirea, distribuirea sau furnizarea, ștergerea sau distrugerea datelor.

Datorită acestei definiții foarte largi, fiecare colecție structurată de date cu caracter personal (dosar electronic și fișier pe hârtie) este afectată fundamental de cerințele legale.

1.4.13 Date personale

Datele cu caracter personal reprezintă orice informație referitoare la o persoană fizică identificată sau identificabilă. Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. Persoanele vizate sunt întotdeauna doar persoane fizice. Persoanele juridice nu sunt acoperite de prevederile de protecție ale Legii privind protecția datelor cu caracter personal. Pe lângă acestea, GRAWE tratează și datele persoanelor juridice cu aceeași grijă și le protejează împotriva accesului neautorizat.

1.4.14 Categorii speciale de date cu caracter personal (date sensibile)

O formă specială de date cu caracter personal sunt date sensibile. Acestea sunt enumerate exhaustiv în Legea privind protecția datelor cu caracter personal și sunt datele persoanelor fizice cu privire la:

- origine rasiala si etnica
- opinie politică
- convingerile religioase sau filozofice
- apartenența socială
- starea de sănătate
- date genetice sau biometrice
- viața sexuală sau orientarea sexuală
- condamnările penale
- măsurile procesuale de constrângere sau sancțiunile contravenționale

Zonă	tip de date sensibile	exemple concrete
Asigurare de viață Asigurare de persoane	Date privind starea de sănătate	Date la semnarea contractului: informații ale persoanei asigurate legate de starea de sănătate sau afecțiuni preexistente, rapoarte medicale pentru evaluarea riscurilor etc. Date la faza de despăgubire: informații despre cazul asigurat (cauza decesului, vătămărilor corporale), rapoarte și constatări medicale etc.
Asigurare de răspundere civilă (vătămări corporale)	Date privind starea de sănătate	Dosar de daune: informații legate de vătămări, rapoarte și constatări medicale etc.
Asigurare de viață Asigurări de persoane Asigurări Auto Asigurări de Bunuri	Date referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale	Dosar de daune: Actele de despăgubire conțin câmpuri prin care se colectează informații ale beneficiarului despăgubirii de asigurare despre faptul dacă a fost sau este subiect al investigațiilor organelor de drept.
Administrarea angajaților	Date de sănătate	Date referitoare la concediile medicale

Tabelul 2: aplicarea datelor cu caracter personal

2. Cuvânt înainte din partea Comitetului de Conducere:

Această politică este folosită pentru a menține funcționarea și utilizarea corectă a tuturor politicilor create pentru companie în ceea ce privește capacitatea de a executa procese TI și protecția datelor, precum și securitatea informațiilor.

Ele sunt o necesitate absolută pentru ca procesele TI să ruleze corect și într-o manieră controlată, cu competența asociată și cu măsurile de securitate necesare.

Pe de o parte, există cerințe care rezultă din legislație, standarde și alte reglementări care trebuie respectate de organizația noastră TI și, prin urmare, sunt descrise în politicile TI. Pe de altă parte, ele servesc ca bază și documentație pentru procesele noastre TI.

Această politică conține în primul rând o descriere a

- Proceselor TI și de protecție a datelor
- competențelor și responsabilităților asociate
- reglementărilor aferente pentru utilizarea infrastructurii TI și
- securității informațiilor.

Astfel, securitatea informațiilor se percepe ca salvgardare a:

- **Confidențialității:** Asigurarea că informațiile sunt accesibile numai utilizatorilor autorizați,
- **Integrității:** Asigurarea corectitudinii și exhaustivității informațiilor și a metodelor de prelucrare,
- **Disponibilității:** Asigurarea faptului că utilizatorii autorizați au acces la informații și la activele aferente, după cum este necesar, în orice moment.

Securitatea în termenii cuprinși descriși mai sus, este o preocupare căreia conducerea companiei și personalul trebuie să îi atribuie un nivel de importanță majoră.

Având în vedere acest lucru, solicităm tuturor destinatarilor acestei politici, în interesul dumneavoastră și în interesul companiei noastre, să citească cu atenție acest document important, și nu numai să se familiarizeze cu reglementările, codurile de conduită, și sfaturile conținute în acesta, dar care ulterior și în orice moment, să acționeze în conformitate cu acesta, să informeze și instruiască angajații din domeniile dumneavoastră de responsabilitate în mod corespunzător, în funcție de cerințele specifice ale departamentelor în care activați.

Securitatea este o valoare la care are dreptul fiecare din noi. Cu toate acestea, această valoare nu există pur și simplu datorită unui sistem. Mai degrabă trebuie dobândită, dezvoltată și protejată cu grijă. Noi toți, indiferent de locul de muncă și de responsabilitatea care ne-a fost atribuită, ne putem însuși gradul de securitate pe care îl considerăm necesar și dezirabil prin participare personală activă.

3. Protejarea datelor

Protecția datelor cu caracter personal și respectarea strictă a reglementărilor relevante privind protecția datelor în GRAWE CARAT Asigurări reprezintă baza esențială pentru încrederea clienților noștri.

GRAWE CARAT Asigurări, în calitate de companie de asigurări, prelucrează date de la, următoarele persoane (subiecții de date):

- Contractanții/Asigurații
- Persoane asigurate
- Persoane păgubite (asigurare de răspundere civilă)
- Beneficiarii de asigurare
- Agenți, brokeri
- Angajații

Angajații pot, în exercitarea atribuțiilor lor, să obțină cunoștințe despre datele personale sau secretele companiei. Toate aceste informații trebuie tratate ca strict confidențiale și fac obiectul Legii privind protecția datelor cu caracter personal, . Legii cu privire la activitatea de asigurare și Codului Civil al Republicii Moldova.

În domeniul protecției datelor, atunci când procesează datele cu caracter personal, GRAWE trebuie să respecte Legea privind protecția datelor cu caracter personal, care conține:

- Reguli pentru prelucrarea datelor cu caracter personal
- Drepturi subiecților datelor cu caracter personal
- Obligațiile GRAWE ca operator de date cu privire la prelucrarea datelor

Angajații sunt, obligați să:

1. Respecte Legea privind protecția datelor cu caracter personal și toate politicile interne.
2. Respecte secretul comercial.
3. Angajații Companiei au obligația de a nu transmite sau utiliza unor terți neautorizați informațiile despre subiecții de date pe care pot lua cunoștință în timpul activității lor profesionale,

În acest capitol al politicii sunt definite toate principiile necesare pentru prelucrarea datelor cu caracter personal în calitate de angajat GRAWE. În caz de îndoieli referitor la siguranța datelor, contactați responsabilul local pentru protecția datelor. De-asemenea orice întrebări referitoare la măsurile tehnice de securitate trebuie adresate la Securitatea TI GRAWE (GRAWE IT-Sec).

3.1 CLASELE DE CONFIDENȚIALITATE

În funcție de sensibilitatea și clasa de protecție a datelor, acestea pot fi împărțite în diferite niveluri de confidențialitate. Pe baza următoarei scheme de clasificare, măsurile de siguranță pentru fiecare clasă trebuie respectate corespunzător. Pentru fiecare clasă se aplică și măsurile de securitate ale nivelurilor inferioare de confidențialitate (pct. 3.3). (De exemplu, pentru clasa 3, să aplice măsuri din clasele 1-3).

Nivel de confidențialitate	**Descriere**	**Exemple**
Clasa 1	Documente publice	• Broșură produs aprobat • informații de pe site • comunicare către mass-media (PR)
Clasa 2	Corespondență internă și documente fără date personale	• politicile interne • organigrame • instrucțiuni • corespondență internă prin e-mail • documente în SharePoint (Intranet) • rapoarte
Clasa 3	Date cu caracter personal	• datele de bază ale clienților (nume, adresă, data nașterii...) polița de asigurare • cereri de asigurare • date despre partenerii de vânzări • date despre partenerii de afaceri • date din contractul individual de muncă fără informații salariale
	Date interne confidențiale ale companiei	• Documente legate de strategia companiei (de exemplu, strategii legate de reasigurare, produse sau marketing) • Rapoarte ale organelor de Conducere • rapoarte de control/audit

		• Prelucrarea extinsă a datelor a sistemelor TI și a rezultatelor acestora (chiar dacă nu este vorba de date personale), de exemplu rapoarte privind clienții • Documentație tehnică privind sistemele TI (de ex. hărți ale rețelei, detalii de configurare)
Clasa 4	Date/informații sensibile despre angajați Informații medicale despre clienți (date de sănătate) Informații ale beneficiarilor despăgubirii de asigurare despre condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale	• dosare de daune care conțin date de sănătate, de exemplu în cadrul asigurărilor de viață și de persoane • dosare medicale • date salariale Acte de despăgubire prin care se solicită inclusiv informații despre faptul dacă beneficiarul asigurării este sau a fost subiect al investigațiilor organelor de drept
	Date interne strict confidențiale ale companiei	• Informații despre vânzările planificate și de achiziții ale companiei • Scrisori/Expedieri ce conțin date sensibile și rapoarte către autoritățile de supraveghere • Prezentările și protocoalele consiliului Societății • Certificate de criptare • Documentația privind incidentele de securitate • Informații privilegiate despre companiile listate la burse de valori • Semnături electronice

Tabelul 3: Clase de confidențialitate

3.2 NOȚIUNI DE BAZĂ PENTRU PRELUCRAREA LEGALĂ A DATELOR CU CARACTER PERSONAL (CLASELE 3 ȘI 4)

Potrivit Legii 133 privind protecția datelor cu caracter personal, datele cu caracter personal pot fi prelucrate numai în conformitate cu anumite principii. În special, orice prelucrare trebuie să se bazeze pe una dintre următoarele baze legale:

Cazuri de prelucrare legală conform GDPR	**Aplicații GRAWE (exemple)**
Prelucrare pe baza consimțământului persoanei vizate	• Prelucrarea categoriilor speciale de date cu caracter personal și/sau în lipsa situațiilor prevăzute la art. 5, alin. (5) al Legii privind protecția datelor cu caracter personal
Prelucrare pentru executarea unui contract sau a obligațiilor precontractuale	• Contracte de asigurare: date referitoare la inițierea contractului, procesarea cererilor, evaluarea riscurilor, managementul contractelor, gestionarea daunelor. • Acord de comision de broker și contracte de agent: date referitoare la calculul și plata comisioanelor

	• Contracte de muncă: date referitoare la administrarea și formarea personalului.
Prelucrare pentru îndeplinirea obligațiilor legale	• Păstrarea conform cerințelor și termenilor legali de păstrare • Obligații de raportare către autorități, de exemplu, autoritatea fiscală, autoritatea de supraveghere etc. • Răspuns la solicitările organelor de drept și judecătorești • prelucrarea datelor legate de combaterea spălării banilor
Prelucrare în scopul intereselor legitime (al GRAWE)	• mail-uri de marketing poștale • Prevenirea fraudei: Interogare / raportare în cadrul sistemului informațional central (ZIS)

Tabelul 4: Aplicații ale prelucrării legale a datelor cu caracter personal

Este important ca amploarea datelor colectate și utilizarea acestora să corespundă întotdeauna cu scopul propus. Orice utilizare în afara acestui scop nu este permisă.

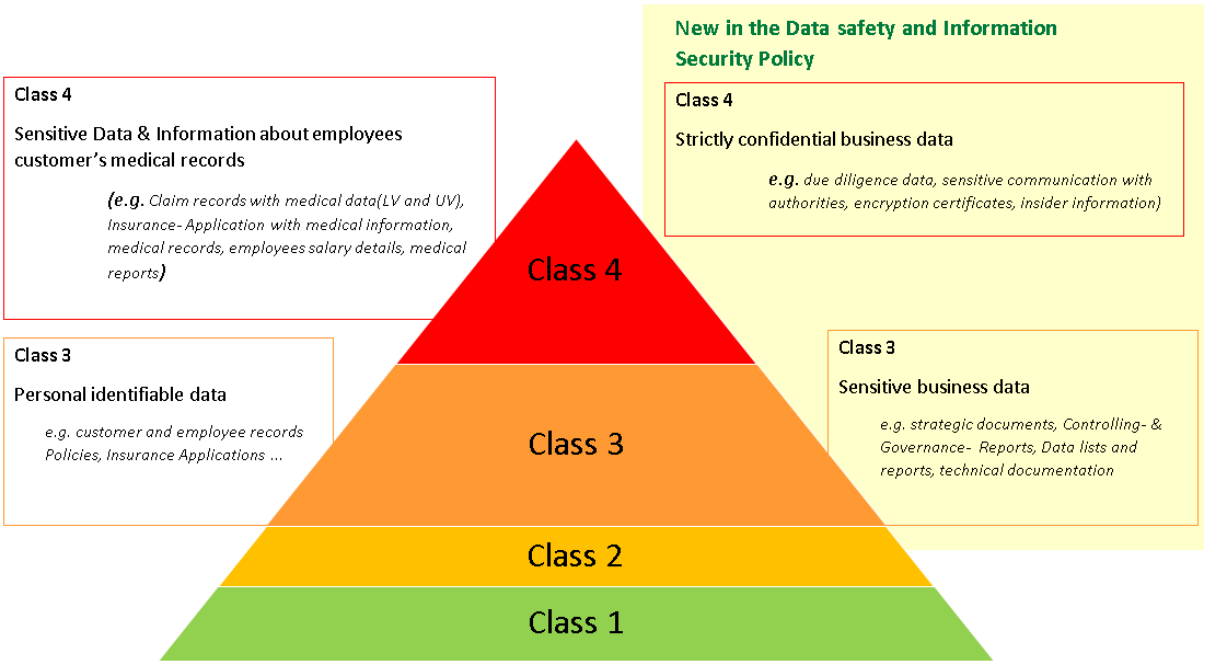
3.3 MASURI DE SECURITATE

Pentru crearea sau modificarea datelor în documente, este necesară și permisă salvarea documentelor de toate nivelurile de confidențialitate pe computerele locale.

Nivel de confidențialitate	**Descriere**
Clasa 1	Nu sunt necesare măsuri de securitate, deoarece datele sunt publice.
Clasa 2	Datele trebuie să fie păstrate în sistemele TI centrale, de exemplu, directoriile departamentelor, SharePoint, etc. Datele de clasa 2 și mai sus pot fi transferate numai către terți autorizați.
Clasa 3 suplimentar	Datele trebuie să fie criptate la salvarea pe suport amovibil (USB, hard/solid state disk-uri externe, etc.). Datele sunt prelucrate și stocate numai în programele respective (directorii și fișiere cu acces restricționat, KORIN, K3, PAM, SAP, sisteme TI a Resurselor Umane, etc.). Datele pot fi create, modificate sau șterse, numai de către angajații cu privilegiile lor respective.
Clasa 4 (sensibil) suplimentar	Datele sunt stocate numai în Sistemele TI a departamentelor Resurselor Umane, KORIN, K3, în Arhiva (PAM) din GRAWE Berater cu partajare cu acces restricționat, în Directoriile serverelor de stocare a datelor. Datele pot fi transmise electronic doar atunci când e garantată transferarea criptată (de exemplu, prin intermediul platformelor web securizate https, SecMail, SSH).

Tabelul 5: Măsuri de securitate legate de nivelurile de confidențialitate

AES-128, RSA-2048, sau mai mare, trebuie să fie utilizate pentru toate tipurile de criptare. Criptarea datelor pe dispozitive de stocare USB, se va efectua folosind funcția „adăugați la arhiva criptată” din exploratorul de ieșire.



3.4 TRANSFER DE DATE CĂTRE TERȚI

3.4.1 Destinatari autorizați

Orice transfer de date personale către destinatari din afara GRAWE, trebuie să fie acoperit de unul dintre temeiurile legale menționate la pct.3.2. Aceasta înseamnă că transferul trebuie să se bazeze pe consimțământ, să fie necesar pentru executarea unui contract sau în baza unei obligații legale.

Exemplu de transferuri „tipice" permise în cadrul activității de asigurări:

Destinatar	Scopul transferului de date
Medici, spitale	Solicitarea dosarelor medicale suplimentare pentru evaluarea riscurilor
Specialiști / experți	Solicitare de rapoarte de expertiză
Reprezentant de despăgubire	Cerere de gestionare a daunelor
Agent	Răspuns la solicitări de informații a unui broker, în baza împuternicirii unui deținător de poliță
Avocat	reprezentarea intereselor Grawe în instanțele judecătorești și alte autorități
Reasigurare	Cerere de evaluare a riscurilor (subscriere), soluționare daune
Instanțele civile	Depunerea declarațiilor terților debitori în cadrul procedurilor de executare
Autorităților publice	Răspuns la solicitările de informații
Administrator al insolvabilității / Lichidator	Răspunsul la solicitările de informații legate de procedura de faliment

Notar	Răspunsul la solicitările de informații legate de procedurile de succesiune

Tabelul 6: Destinatari autorizați

3.4.2 Transferul datelor speciale

Angajații sunt obligați ca datele cu caracter personal speciale să fie transferate în unul dintre următoarele moduri:

- Poștale, fizice
- e-mail criptat, conform Ghidului privind email-ul securizat
- portaluri online securizate

In cadrul GRAWE, se aplică următoarea cerință pentru transferurile prin e-mail:
Nu se admite expedierea datelor despre sănătate necriptate, la o altă adresă de e-mail decât prenume.nume@grawe.md.

3.4.3 Informațiile furnizate în timpul anchetelor telefonice

În cazul în care un apelant telefonic solicită informații specifice privind contractele de asigurare, apelantul trebuie să fie mai întâi identificat.

Principial, informațiile prin telefon pot fi acordate exclusiv persoanei vizate. Adițional la numele apelantului, se vor solicita informații suplimentare cu caracter personal verificabile, care pot fi oferite doar de către client, cum ar fi, numărul de poliță deținută, IDNP-ul, numărul cererii de despăgubire sau ID-ul de client. Alternativ, clientul va fi apelat înapoi la numărul de telefon stocat în KORIN / K3.

Dacă apelantul se identifică ca reprezentant al clientului, prezența unei procuri valabile și conținutul acesteia trebuie întotdeauna verificate înainte de a fi furnizate orice informații.

3.5 DREPTURILE PERSOANELOR VIZATE

În baza Legii 133 privind protecția datelor cu caracter personal, persoanele vizate au drepturi diferite pe care le pot exercita:

Drepturile subiecților	Conținut
Dreptul de informare	Operatorul de date cu caracter personal are obligația la solicitare să furnizeze informații cu privire la: identitatea operatorului, scopul prelucrării, destinatarii datelor, dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sânt obligatorii sau voluntare, precum și consecințele posibile ale refuzului de a răspunde
Dreptul de acces	Persoanele vizate au dreptul de a obține informații despre care dintre datele lor personale sunt prelucrate, principiile de funcționare a mecanismului prin care se efectuează prelucrarea datelor cu caracter personal, consecințele juridice generate de prelucrare, modul de exercitare a dreptului de intervenție.
Dreptul de a revoca	În cazul în care prelucrarea datelor se bazează pe un consimțământ, acest lucru poate fi revocată în orice moment. O astfel de revocare intră în vigoare imediat, dar nu și pentru activitățile anterioare.
Dreptul la ștergere	Persoanele vizate pot solicita ștergerea datelor prelucrate contrar Legii 133 (de exemplu, prelucrarea datelor fără un temei legal).
Dreptul la rectificare	În cazul în care datele sunt prelucrate incorect sau incomplet, ori sau – modificat, persoana vizată poate solicita corectarea acestor date.

Dreptul la restricționarea prelucrării	În cazul în care nu este clar dacă datele unui subiect de date sunt incorecte, sau incomplete, sau în cazul în care prelucrarea datelor este ilegală, persoana vizată poate solicita o restricție a prelucrării datelor până la clarificarea situației sau corectarea datelor dacă e cazul.

Tabelul 7: Drepturile persoanelor vizate

La o solicitare prin care persoana vizată își exercită unul dintre drepturile menționate, i se va răspunde în termen de 30 zile de la primirea solicitării.

ATENȚIE : Persoanele vizate își pot exercita drepturile în orice tip de corespondență și comunicare (de exemplu scrisori de reziliere, cereri de daune).

Orice angajat este obligat să transmită responsabilului de protecția datelor solicitările exercitate în orice mod (scris, prin e-mail) referitor la un drept vizat menționat mai sus, prin intermediul e-mailului dcp@grawe.md.

Excepție: Dreptul de rectificare trebuie să fie realizat de către angajații responsabili de operarea datelor de acest tip, în procedură obișnuită (de exemplu, introducerea unei noi adrese, schimbarea numelui, etc.).

3.6 ETICHETAREA INFORMAȚIILOR

Documentele pot fi etichetate în funcție de nivelul confidențialitate. Eticheta trebuie să fie clară pentru fiecare nivel de confidențialitate și evidentă pe documentele tipărite și digitale. Documentele care sunt transferate către terți și cele care sunt clar identificabile ca ne-apartenente unui anume nivel de confidențialitate (de exemplu, materiale de marketing, fluturași, marketing legat de clienți, etc.) nu necesită etichetare. Acest lucru se aplică și documentelor de lucru, listelor neformatate, rapoartelor tehnice, jurnalelor/log-urilor, etc.

Toate documentele care nu sunt etichetate trebuie privite ca documente de clasa II – interne.

3.7 FURNIZORI SAU CONTRACTORI TI

Orice antreprenor TI sau furnizor TI trebuie să fie înregistrat în registrul de furnizor în sistemul de tichete TI (http://it.grawe.at). Contractanții sau furnizorii TI, care urmează să fie angajați, înainte de angajarea lor, urmează să fie raportați prin intermediul sistemului informatic de tichete (http://it.grawe.at); acest lucru se va face fie prin coordonatorul TI al departamentului respectiv sau prin administratorul TI local. Pentru raportarea noilor contractanți sau furnizori, se va completa articolul corespunzător „furnizor sau furnizor de servicii TI nou“, cu informații de baza a contractatului, clasificând furnizorul (a se vedea *Tabelul 8*) și persoana responsabilă din cadrul TI. Această procedură asigură că toți contractorii și furnizorii TI sunt înregistrați în registrul central.

În cazul în care datele personale sunt transmise de către GRAWE către contractorul TI, sau furnizorul TI (TIP 2) pentru prelucrare, sau în cazul în care contractantul TI, sau furnizorul TI este autorizat să acceseze sistemele TI GRAWE (TIP 3), se va încheia un contract de prelucrare a datelor conform GDPR. Coordonatorul TI al departamentului respectiv, sau administratorul TI local, trebuie să contacteze coordonatorul pentru protecția datelor la GRAWE, înainte de a încheia acel acord de prelucrare a datelor.

Un șablon de acord de prelucrare a datelor în limba germană și limba engleză este disponibil la SharePoint la (https://sharepoint.grawe.at/abteilungen/GD_IT/IT_Prozessdokumentation/Richtlinien) și se va adaptă și/sau traduce după caz.

TIP	Descriere	Măsuri	Acord de procesare a datelor semnat
1	Contractor TI sau furnizor TI care nu primește date personale de la GRAWE și care nu are acces la sistemele TI interne	Înregistrarea la registrul central.	Nu este necesar

	ale GRAWE (cum ar fi un furnizor de hardware)		
2	Contractor TI sau furnizor TI care primește date personale de la GRAWE, dar nu are acces la sistemele TI interne ale GRAWE	Înregistrarea la registrul central. Copie a contractului de prelucrare a datelor semnate salvate în registrul contractant TI centrale / furnizor Revizuirea anuală dacă serviciile TI contractant / furnizor sunt încă necesare	Necesar
3	Contractor TI sau furnizor TI cu acces autorizat la sistemele TI interne GRAWE		

Tabelul 8: Prezentare generală a tipurilor de contractori TI sau furnizori TI

4. Locul de lucru

Angajatului GRAWE CARAT Asigurări, i se va pune la dispoziție un loc de muncă modern, din punct de vedere TI, potrivit pentru munca angajatului destinat exclusiv în scopuri de serviciu. Produsele hardware și software la GRAWE sunt cumpărate și/sau utilizate exclusiv după consultarea GRAWE IT Services.

Utilizatorul este responsabil pentru utilizarea corectă a dotărilor TI furnizate. Dispozitivele transportabile trebuie păstrate întotdeauna în siguranță, obligatoriu împiedicând orice acces a terților la dotările/echipamentele/bunurile/aplicațiile oferite de GRAWE. Utilizarea corectă este monitorizată în mod regulat în cadrul sistemului de control (ICS) intern al GRAWE IT Services.

4.1 ACHIZITII HARDWARE-ULUI LA GRAWE

Hardware-ul este achiziționat exclusiv prin intermediul departamentului TI local și va corespunde criteriilor și specificațiilor TI ale Grupului, care asigură capacitatea de administrare și securitatea totalității sistemelor GRAWE. Reparațiile hardware sunt efectuate sau contractate exclusiv de departamentul TI local.

4.2 CONECTAREA HARDWARE-ULUI NON-GRAWE

Conectarea și operarea hardware-ului este interzisă fără aprobarea Serviciului TI al Grupului GRAWE. Aceasta include, dar nu se limitează la următoarele:

- Conectarea notebook-urilor personale/non-GRAWE, a tabletelor PC sau a unităților desktop/tower (PC-uri) și a echipamentelor periferice ale acestora la rețeaua GRAWE.
- Conexiunea dispozitivelor personale, sau non-GRAWE de rețea, cum ar fi routere Wi-Fi, imprimante, etc la rețeaua GRAWE.
- Utilizarea stick-urilor de internet mobil/modemelor incorporate, în timp ce dispozitivul este conectat la rețeaua GRAWE.
- Punerea în funcțiune hardware sau software în cadrul rețelei GRAWE.

Utilizarea dispozitivelor de stocare private/non-GRAWE (hard disk-uri, stick-uri USB, purtătoare de informații/media optice) cu hardware GRAWE este permisă numai atunci când:

- este folosit în scopuri profesionale
- utilizarea dispozitivelor GRAWE deținute, nu este posibilă,
- angajatul este convins că utilizarea acestui dispozitiv nu reprezintă un risc de securitate pentru infrastructura TI GRAWE, în plus, nu există nicio suspiciune de software rău intenționat pe dispozitiv.

Soluția de securitate antivirus documentează cazurile când datele companiei sunt copiate pe un mediu amovibil, pe care calculator sa efectuat copierea acestora sau dacă orice hardware care este diferit de standardul companiei este conectat la dispozitivul dumneavoastră.

4.3 CONFIGURAREA SISTEMULUI DE OPERARE

Se va folosi un sistem de operare, care Serviciul TI de Group l-a testat pentru compatibilitate. În funcție de oportunități și necesitate, versiuni mai noi atât a sistemului de operare, precum și a software-ului instalat, va fi instalat centralizat. Software-ul este instalat pe computer exclusiv de unitatea TI locală. Datele de pe unitățile de stocare a informației interne, sunt criptate în mod implicit (criptarea întregului disc).

Modificările configurației computerului (hardware-ului și software-ului GRAWE), care sunt efectuate de altcineva decât departamentul TI local, pot duce la consecințe imprevizibile în rețea, care afectează toate sistemele GRAWE Group. Prin urmare, utilizatorii nu au voie să facă modificări neautorizate în configurația computerului sau să instaleze aplicații. Acest lucru nu este posibil și din motive legale, de licențiere, și de asemenea pentru asigurarea securității sistemelor GRAWE.

Orice încercare de a ocoli măsurile de securitate ale computerelor sau rețelelor, va fi privită ca abatere disciplinară și în consecință pedepsită.

Aceasta include, dar nu se limitează la:

- încercare de descoperire sau spargere a parolelor;
- instalare de software care are ca scop ocolirea prezentei politici;
- pornirea unui computer GRAWE de pe un dispozitiv extern/terț, adică nu de pe dispozitivul local configurat de serviciul TI;
- dezactivarea permanentă a protecției antivirus sau a paravanului de protecție local.

Toate incidentele care indică faptul că securitatea sistemelor și/sau a rețelelor, ar putea fi expuse riscurilor, vor fi imediat raportate la Serviciul TI al Grupului GRAWE.

4.4 DREPTURILE DE UTILIZARE

Toate tipurile de echipamente/infrastructură TI, care sunt utilizate de către angajat, sunt disponibile numai în scopuri profesionale și în limitele capabilităților tehnice. Dreptul de utilizare poate fi retras de GRAWE. Prin urmare, utilizatorii nu pot obține drepturi permanente pentru serviciul oferit și nu pot fi formulate niciun fel de pretenții. În plus, GRAWE exclude răspunderea, în măsura în care este permisă de lege, pentru orice daune legate de utilizarea hardware-ului, software-ului sau a rețelei GRAWE.

4.5 PIERDERI

În calitate de utilizator al hardware-ului companiei, cum ar fi un notebook, un computer sau un smartphone, sunteți responsabil pentru păstrarea în siguranță a echipamentului companiei. Poliția trebuie anunțată în consecință în cazul în care dispozitivul dumneavoastră este furat sau pierdut. O copie a raportului trebuie pusă la dispoziția GRAWE CARAT Asigurări.

Informați imediat TI-ul local despre pierderea sau furtul unui dispozitiv, în special al unui dispozitiv mobil (smartphone, token, notebook), deoarece echipamentul pierdut poate reprezenta un risc de securitate pentru întreaga infrastructură GRAWE. Procedura în cazul pierderii hardware-ului mobil este următoarea:

O pierdere eventuală trebuie raportată imediat TI-ului local, astfel încât accesul neautorizat la sistemele GRAWE să poată fi blocate imediat.

Departamentul TI local poate fi contactat în timpul orelor de muncă. Notificarea se va efectua prin e-mail la admins@grawe.md, sau telefon (+373 2222 9299).

Ulterior, TI-ul local va informa entitățile ce urmează a fi notificate sau implicate.

Dacă notificarea de către utilizator întârzie, atunci utilizatorul este responsabil pentru orice daune apărute în consecința nerespectării obligației de notificare.

4.6 DETERIORAREA

Echipamentul companiei nu va fi deteriorat și nu vor fi aplicate etichete/abțibilduri private.

TI-ul local trebuie informat imediat în cazul oricărei deteriorări a resurselor TI (hardware, software) pentru a evita orice daune în consecința deteriorării și ne-reparării prompte. Fiecare utilizator este răspunzător pentru orice daune provocate din culpă sau inacțiune.

4.7 UTILIZAREA ÎN AFARA SEDIILOR GRAWE

Această politică trebuie menținută și în afara sediilor GRAWE. În acest caz, sunt aplicate următoarele reguli:

- Hardware-ul, software-ul și toate/orice date, pot fi folosite în afara GRAWE cu autorizare prealabilă, cu excepția că necesitatea e dictată de activități de afaceri (de exemplu, vizite la client, etc.) sau care corespunde scopului dispozitivului specific (de exemplu, telefoane, laptop-uri, etc.)
- Dispozitivele nu vor fi lăsate nesupravegheate în zonele de acces public.
- Dispozitivul va fi utilizat exclusiv de un angajat GRAWE.

4.8 END-USER COMPUTING [1]

Sculele End-user computing reprezintă diverse aplicații și programe individuale, ce pot fi utilizate, dezvoltate sau operate de utilizatorii finali din afara departamentului TI. Acestea nu includ doar aplicații standard, ci și aplicații dezvoltate personalizat, cum ar fi macro-comenzi în registrele de lucru Excel. Destinația unor astfel de aplicații e de a completa/asista procesele esențiale de business.

Asemenea aplicații trebuie să fie raportate și actualizate în registrul central IDV în SharePoint-ul GRAWE de către coordonatorii TI din departamente, sau în lipsa lor, de către responsabilii TI locali. În timpul procesului de înregistrare se efectuează o evaluare a riscurilor, din care rezultă dacă trebuie aplicate careva măsuri suplimentare.

5. ID de utilizator și parolă

Fiecare sistem TI GRAWE este protejat cu un ID de utilizator și o parolă pentru a preveni utilizarea necorespunzătoare, inclusiv de către terți. Este interzisă transmiterea parolelor colegilor sau altor terți. Dacă, din motivele expuse mai sus, o terță parte provoacă daune cu ajutorul ID-ului dvs. de utilizator, atunci utilizatorul al cărui ID a fost folosit este solidar responsabil pentru orice daune și consecințe.

În niciun caz, ID-urile de utilizator sau parolele nu trebuie păstrate cu neglijență, cum ar fi sub tastatură sau în locuri banale (de exemplu, note lipite sub/pe birou, sau echipamente).

Dacă există suspiciune că o parolă a devenit cunoscută altor persoane, aceasta trebuie schimbată imediat de utilizator, sau ultimul poate solicita ajutorul departamentului TI local.

Fiecare utilizator trebuie să se autentifice cu ID-ul de utilizator alocat (nu sunt permiși utilizatorii colectivi) și să se deconecteze utilizatorul autentificat (Sign off) la părăsirea locului de muncă.

Fiecare stație de lucru se blochează automat dacă un utilizator este inactiv mai mult de 30 de minute. Computerul trebuie să fie blocat (Lock) atunci când este lăsat fără supravegherea utilizatorului. Procedura de deconectare (Logoff), se va efectua obligatoriu de utilizator în toate cazurile de absențe provizorie. În cazuri justificate, departamentul TI poate forța un logoff dacă un utilizator este absent și nu s-a deconectat.

O parolă poate fi resetată doar de către utilizator și o resetare a parolei poate fi solicitată numai de către utilizator însuși.

[1] Politica Grupului GRAWE pentru End-User Computing:
https://sharepoint.grawe.at/abteilungen/GD_IT/IT_Prozessdokumentation/Richtlinien/Forms/AllItems.aspx

5.1 POLITICA PAROLELOR

O parolă trebuie să aibă cel puțin 12 caractere pentru utilizatori și 15 caractere pentru administratori și personalul TI. Angajații vor folosi doar parole de acces sigure. O parolă trebuie să satisfacă următoarele criterii:

Descriere:	Valori:
Valabilitatea maximă a parolei	90 de zile
Istoricul parolelor (numărul de parole anterior utilizate nepermise)	24
încercări de introducere a unei parole greșite până la blocarea utilizatorului	5 încercări de conectare nereușite
Se deblochează automat după	15 minute

Tabelul 9: Pas SWO Politica rd

- litere mari (A - Z)
- litere mici (a - z)
- numere (0 - 9)
- Nu pot fi folosite caractere specifice limbii/diacritice, cum ar fi Ă, Î, Â, Ş, Ţ, Š, Ž, ć, ü, ö, ä, ß, ă,î,â,ş,ţ.
- Parola nu trebuie să conțină nicio caracteristică cunoscută, cum ar fi, de exemplu, un nume, un prenume, ziua de naștere, modelul de mașină, date ușor deductibile, nume a lunilor și anul, etc.
- Nu pot fi utilizate modele/șabloane de tastatură (de ex. asdfg, qwerty, etc.)
- Inadmisibilă găsirea unei parole în formă neschimbată într-un dicționar sau enciclopedie.

Modificările trebuie să afecteze întreaga parolă și nu doar caracterele individuale (HolidayKreta**2010** în loc de HolidayKreta**2011** nu este permis).

Parolele inițiale sunt individuale pentru fiecare utilizator. Acestea vor fi obligatoriu modificate la prima încercare de conectare a utilizatorului.

Conturile de utilizator tehnice (SRV_, RES_) nu au o perioadă definită de valabilitate a parolei. Din cauza incompatibilități tehnice, trebuie evitate parole mai lungi de 24 de cifre.

5.2 AUTENTIFICARE CU DOI FACTORI (GRIDTOKEN, IT-SUDOKU)

Pentru accesarea sistemelor interne din afara rețelei GRAWE, pe lângă numele de utilizator și parola se aplică un factor de securitate suplimentar, așa-numitul GridToken.

Descriere:	Valoare:
Mărimea minimă a simbolului	6 cifre
Încercări greșite până la blocarea utilizatorului	6 încercări de conectare nereușite
Se deblochează automat după	15 minute.

Tabelul 10: Criterii pentru GridToken

6. Informații - Incidente și puncte slabe de securitate

Un incident de securitate a informației este o abatere a procedurilor zilnice de afaceri, care indică faptul că politica de securitate sau măsurile de securitate au fost încălcate. Chiar și suspiciunea de încălcare a unei politici trebuie văzută ca un incident de securitate.

Pentru izolare, este necesară detectarea și identificarea rapidă ca incident de securitate.

În cazul oricărui incident de securitate, sprijinul angajatului afectat este crucial. TI-ul local își rezervă dreptul de a analiza conformitatea sau posibila utilizare greșită a dispozitivului afectat împreună cu angajatul afectat. Prin urmare, GRAWE este autorizat să analizeze toate datele de pe dispozitiv pentru a analiza, atenua și conține incidentul de securitate a informațiilor.

6.1 DETECTAREA INCIDENTELOR DE SECURITATE

Incidentele de securitate a informațiilor apar sub diferite forme, prin urmare sunt enumerate următoarele exemple de incidente de securitate. Acest lucru ar trebui să fie văzut ca un ghid brut, nu ca o specificație exactă.

- Pierdere sau furt de hardware, software sau date
- Virus
- E-mail de phishing reușit
- Sabotaj al sistemelor
- privilegii nelegitimate ale utilizatorului/utilizatorilor
- Partajarea parolei
- Tratarea neautorizată a datelor (de exemplu, redirecționarea neintenționată a e-mailurilor către destinatari greșiți.)
- Dispozitive TI necunoscute din rețea (de exemplu, PC-uri sau dispozitive necunoscute, puncte de acces etc.)
- Inginerie socială (o persoană necunoscută încearcă să obțină informații)
- Încălcarea politicii de securitate
- Alte evenimente din domeniul Securității Informației
- etc.

6.2 RAPORTAREA INCIDENTELOR DE SECURITATE

Suspiciunea unui incident de securitate trebuie raportată imediat departamentului TI-ului local. Departamentul TI local este disponibil în timpul orelor de serviciu.

Canale posibile de raportare:

- Tichet pe portalul Hotline IT-Service - „Raportați incident de securitate” http://it.grawe.at
- E-Mail la admins@grawe.md, sau în caz de imposibilitate/aflare peste hotarele țării, la hotline@grawe.at
- Telefon +373 2222 9299, sau la aflarea în afara țării, la +43 316 908031 8888

Departamentul TI local efectuează verificarea suspiciunilor și întreprinde măsuri corespunzătoare.

6.3 DETECTAREA ȘI RAPORTAREA DEFICIENȚELOR DE SECURITATE A INFORMAȚIILOR

Vulnerabilitățile din domeniul securității informațiilor pot fi fie vulnerabilități tehnice, fie drepturi de acces neautorizate/excesive la sisteme, sau deficiențe organizaționale a procedurilor sau proceselor.

Exemple pentru vulnerabilități tehnice:

- software vechi sau neactualizat
- configurație defectuoasă a sistemului
- privilegii extinse în sistemele GRAWE, care nu sunt necesare utilizatorilor pentru exercitarea obligațiilor funcționale.
- etc.

Exemple de vulnerabilități ale organizației:

- informațiile confidențiale sunt disponibile pe coridoare sau la imprimante
- informațiile confidențiale sunt aruncate în coșul de gunoi și nu sunt distruse
- etc.

Suspiciunile de deficiențe în securitatea Informațiilor trebuie raportate imediat prin utilizarea portalului de servicii TI (http://it.grawe.at) și intrarea corespunzătoare „Raportați deficiențe în Securitatea Informațiilor”/“Report Information-Security Weakness”.

7. Programe malware

TI-ul local va instala implicit un scanner de viruși de Serviciul TI de Group, pe fiecare computer din GRAWE. Acesta va fi ținut la zi automat și va fi actualizat centralizat, cu noi fișiere de definire a virușilor. Utilizatorului nu i se

permite să oprească acest program sau să-l dezinstaleze. Cu toate acestea, infecțiile sunt încă posibile prin fișiere de pe stick-uri USB, CD-uri sau alte medii prin descărcări și prin laptopuri care se conectează la Internet în afara rețelei GRAWE.

Rețeaua GRAWE este protejată în mai multe nivele împotriva malware.

Chiar dacă se recepționează un e-mail de la expeditori presupus cunoscuți sau de încredere, trebuie să verificați dacă textul din mesaj se potrivește și cu expeditorul (spre exemplu text în engleză de la persoana de contact vorbitoare de germană sau română, text îndoielnic sau lipsă de referință la evenimente specifice, lipsa unui subiect business sau a unui subiect semnificativ, etc.) și dacă atașamentul era așteptat/se presupune să fie prezent în acel e-mail.

Nu aveți încredere în e-mailurile de la expeditori necunoscuți, atașamente sau site-uri web. Solicitările de descărcare, modificarea setărilor, introducerea parolelor, deschiderea atașamentelor trebuie analizate foarte critic.

Utilizarea fișierelor de aplicații (* .COM, * .exe, etc.) sau limbaje de scripting (* vbs, * .BAT, etc.) este permisă numai în scop de afaceri și în cazul în care nu există nici o dovadă a unui risc de securitate pentru infrastructura TI GRAWE, în plus, în cazul în care nu există nici o cale spre cod rău intenționat în atașament. De asemenea, se va manifesta prudență cu documente Office (* .doc, * .xls * .PPT, * .PDF, etc.) și screensavere. (* .SCR etc.) fie din Grup sau din afara Grupului GRAWE.

Dacă un virus este nou, este posibil ca acesta să nu fie detectat prin proceduri de testare standard. Din acest motiv, atașamentele suspecte sunt șterse automat, cu excepția fișierelor ZIP. Ultimele sunt doar validate. Prin urmare, atașamentele din fișierul ZIP trebuie tratate cu mare grijă și critic.

Un e-mail în format HTML poate conține și conținut activ cu funcții dăunătoare. Pentru a proteja împotriva virușilor de poștă HTML, modul de previzualizate ar trebui să fie dezactivat în clientul de e-mail (Outlook), deoarece codul rău intenționat poate fi în corpul e-mailului și ar putea fi activat de pre-vizualizare.

8. Utilizarea internetului și a e-mailului

Internetul cu rețeaua sa de servicii World Wide Web (WWW) și e-mail-ul, sunt un mijloc de informare și comunicare, care pot contribui într-o mare măsură la optimizarea activităților de afaceri. Prin urmare, Internetul este o resursă importantă, și cât mai mulți angajați GRAWE profită utilizându-le. Următoarele politici privind utilizarea internetului au fost definite pentru toți utilizatorii GRAWE, în scopul de a crea claritate și pentru a preveni un potențial abuz.

8.1 UTILIZARE

Utilizarea Internetului în cadrul rețelei GRAWE și a adresei de e-mail GRAWE este exclusiv în scopuri profesionale. Serviciul TI al Grupului folosește software de filtrare pentru a bloca accesul la anumite site-uri web, care sunt de obicei utilizate numai în scopuri private. Accesul la Internet este înregistrat pentru sisteme individuale în GRAWE. Accesul la Internet din interiorul rețelelor este posibil numai pentru utilizatorii GRAWE, prin intermediul proxy-ului web GRAWE, utilizând browserul web implicit definit. Stocarea acreditărilor (nume de utilizator sau parolă) în browser nu este permisă.

Astfel, este interzisă accesarea sau difuzarea unui conținut definit ca:

- rasist (ce include conștientizarea rasială exagerată și rasismul),
- sexistă (aceasta include activități și comentarii care vizează discriminarea persoanelor din cauza sexului lor),
- discriminatorie (prejudicierea imaginii și reputației părții afectate prin efectuarea de comentarii sau declarații inexacte în public sau prin dezavantajarea acestor persoane printr-un tratament diferit);
- sau care glorifica violenta.

În același mod, sunt interzise toate activitățile care pot afecta reputația GRAWE și/sau pot dăuna imaginii acesteia.

De asemenea, orice utilizare potențial ilegală sau relevantă pentru drepturile de autor a internetului sau a e-mailului (vânzare, distribuire sau stocare de pornografie infantilă sau conținut nazist, piraterie de software...) este strict interzisă. GRAWE este obligat să ofere sprijin nerestricționat autorităților pentru clarificarea infracțiunilor și va urmări penal orice utilizare potențial infracțională detectată, cu sesizarea departamentului legal și HR, și consiliului de conducere a întreprinderii.

Descărcarea fișierelor audio și video care nu sunt relevante pentru companie, precum și utilizarea serviciilor de streaming sunt în general interzise. Acestea includ sisteme precum YouTube și radio prin internet.

Utilizarea sistemelor de backup online, pentru stocarea datelor personale precum Dropbox, Microsoft OneDrive etc. este interzisă.

8.2 EXCEPȚII PENTRU ACCESUL LA INTERNET

Dacă, din cauza cerințelor de profesionale, accesarea unui site web blocat este inevitabilă, aceasta se va justifica superiorului dumneavoastră. Dacă autorizarea este oferită de către superior și reprezentantul HR, atunci aceasta trebuie transmisă în scris Serviciului TI al Grupului GRAWE, sau prin ”IT Hotline”. Excepția va fi adaptată în mod corespunzător, iar autorizația va fi documentată.

8.3 CERINȚE PENTRU ANGAJATI LA UTILIZAREA SERVICIILOR DE VIDEOCONFERINȚA

Standarde pentru conferințe video sunt definite în cadrul GRAWE. Licențe și condiții prealabile data safety sunt oferite. Punerea în aplicare a oricărei alte soluții de conferințe video este interzisă.

Următoarele cerințe de bază trebuie să fie respectate:

- Dacă sunteți invitat la o videoconferință externă găzduită de o parte externă, este legitim să utilizați soluția furnizată extern. Dacă este nevoie să instalați software-ul pe computer, contactați departamentul TI local pentru asistență.
- Microfonul va fi dezactivat la intrarea într-o cameră virtuală
- Verificați imaginea video pentru obiecte din cameră care nu ar trebui să fie văzute, înainte de inițierea camerei video.
- Software-ul de conferințe video sau WebBrowser instalate și actualizate de către departamentul TI local, nu vor fi schimbate complet sau pe părți, și nu se vor schimba configurațiile.
- Salvarea videoconferinței fără aprobarea tuturor participanților este interzisă.
- Folosind un chat paralel cu videoconferința, comportă-te astfel încât orice fel de publicare a conținutului să nu poată dăuna ție sau companiei.

Precauții suplimentare pentru organizatorii de conferințe

- În calitate de organizator (expeditor al invitației) sunteți responsabil pentru buna desfășurare a conferinței.
- Verificați în prealabil dacă sunt disponibile și suficiente modalitățile de participare selectate (de exemplu, telefon) pentru scopul conferinței.
- În calitate de organizator, verificați toți participanții. Dacă un participant neinvitat accesează conferința, opriți conferința și cereți persoanei să părăsească conferința, sau excludeți-o dacă refuză.

9. Protecție fizică

9.1 DATE TIPĂRITE

O copie tipărită a datelor este adesea făcută pentru prelucrare ulterioară. Copiile pe hârtie și suporturile de date (CD-uri, DVD, unități USB etc.) trebuie să fie manipulate în conformitate cu confidențialitatea și importanța datelor pe care le conțin.

Nu lăsați nicio informație sensibilă tipărită accesibilă în mod liber

Aruncați orice informație sensibilă tipărită în containerele securizate, sau distrugătoare de hârtie și suporturi media (shredder). Nu folosiți coșul de gunoi obișnuit.

9.2 FOLDERE

Este obligatoriu ca folder-ele cu acumulări mari de date personale sau chiar sensibile să fie păstrate în cutii sub cheie. Nu este permisă depozitarea permanentă într-o zonă liber accesibilă.

9.3 PERSOANE EXTERNE

Urmăriți persoanele externe/terțe, care le întâlniți în holuri, camere sau birouri, și care nu sunt însoțite de un angajat GRAWE cunoscut. Verificați identitatea sau afilierea la GRAWE a persoanelor care Vă sunt necunoscute.

În general, observați că persoanele externe, clienții și angajații neautorizați nu trebuie să aibă acces la următoarele zone:

- Zone de încasare / flux de numerar
- ID
- Inspectare de autovehicule
- Dulapuri de rețea, mufe de rețea, dispozitive de rețea
- Notebook-uri, PC-uri și smartphone-uri
- Dosare, oferte, notificări de revendicare, dosare de daune
- Camere de server și facilități de rețea
- Camere de administratorii TI

10. Informații - Securitate în situații de urgență

În cadrul GRAWE se stabilește un Management al Continuității Afacerii (BCM), care definește procesele în timpul unei situații de urgență. Procesele inter-companii referitoare la BCM sunt gestionate de departamentul central de management al riscurilor.

O urgență în cadrul companiei, este orice eveniment cu impact negativ major, care oprește procesele obișnuite de afaceri pentru toată compania, sau o parte a companiei, pentru o anumită perioadă de timp. Dacă există vreun eveniment major, membrii comitetului de conducere declară starea de urgență.

În timpul unei urgențe, toate reglementările acestei politici de securitate a informației și orice alte politici TI trebuie respectate necondiționat.

Dacă sunt necesare măsuri specifice situației, angajații vor fi informați detaliat în prealabil.

Toate tipurile de comunicare externă (de exemplu, presă, mass-media, autorități) sunt făcute numai de comitetul de conducere, sau sunt cel puțin aprobate de comitetul de conducere. Solicitarea din partea presei / mass-media trebuie refuzată și trebuie redirecționată către canalele de comunicare responsabile ale companiei.