

Anexa 17 Securitatea Informațiilor

1 Cerințe privind Securitatea Informațiilor

Cerințele globale sunt cerințe care se aplică, în general, furnizării tuturor serviciilor de către furnizor.

- 1.1 Surse recunoscute:** Furnizorul se asigură că produsele hardware și software sunt obținute din surse cunoscute și renumite și că există un suport tehnic fiabil și un lanț de aprovizionare trasabil.
- 1.2 Guvernanța în domeniul securității:** Furnizorul stabilește, menține și monitorizează un cadru de guvernanță în materie de securitate a informațiilor, care permite organului de conducere al furnizorilor să stabilească o direcție clară și să demonstreze angajamentul său față de securitatea informațiilor și gestionarea riscurilor.
- 1.3 Managementul Riscurilor Informaționale:** Furnizorul se asigură că (i) înainte de implementarea unor noi medii IT care găzduiesc informații ale DELGAZ GRID, (ii) înainte de implementarea unor modificări majore la cele existente, și (iii) introducerea unor noi tehnologii semnificative, riscurile de securitatea informației asociate sunt evaluate, tratate, monitorizate și păstrate în limite acceptabile. Informațiile referitoare la activitățile de gestionare a riscurilor sunt partajate fără întârziere cu DELGAZ GRID, la cerere.
- 1.4 Managementul Securității:** Furnizorul (i) a stabilit o funcție de specialist în securitatea informațiilor, condusă de un manager cu puteri decizionale suficiente, căruia îi sunt încredințate autoritatea și resursele adecvate pentru a asigura aplicarea eficientă și consecventă a bunelor practici privind securitatea informațiilor în întreaga companie și pentru a asigura respectarea cerințelor juridice, de reglementare și contractuale care afectează securitatea informațiilor. Furnizorul (ii) menține un program cuprinzător, actualizat de conștientizare în domeniul securității, pentru a promova și a integra comportamentul așteptat privind securitatea în raport cu toate persoanele care au acces la informațiile DELGAZ GRID.
- 1.5 Proceduri Operaționale Documentate:** Furnizorul a stabilit responsabilități și proceduri pentru administrarea și operarea serviciilor sale pentru a se asigura că această documentație este (i) conformă cu standardele din industrie și bunele practici recunoscute, (ii) documentată în mod adecvat în scris și (iii) actualizată în orice moment în cursul aplicării prezentului Acord. Documentația privind procedurile de operare va fi partajată cu DELGAZ GRID la cerere, fără întârziere.
- 1.6 Managementul activelor:** Furnizorul se asigură că (i) activele (hardware și software) care sunt folosite pentru a crea, procesa, stoca sau transmite informații DELGAZ GRID sunt protejate împotriva corupției, pierderilor, furtului și divulgării neautorizate pe tot parcursul ciclului lor de viață. Furnizorul se asigură că aceste active sunt înregistrate într-un registru care este (ii) protejat împotriva modificărilor neautorizate, (iii) actualizat, (iv) copiat periodic (backup) și (v) conține detaliile necesare privind activele hardware și software și include - dacă este cazul - cerințele de conformitate referitoare la active. Furnizorul se asigură că (vi) toate activele sunt alocate unui proprietar care este responsabil pentru operarea (exploatarea) activului.
- 1.7 Accesul la sistem:** Furnizorul restricționează accesul la activele în care informațiile DELGAZ GRID sunt create, procesate, stocate sau transmise persoanelor autorizate în

scopuri comerciale specifice. Aceasta include cel puțin faptul că (i) doar utilizatorii autorizați pot avea acces la informații relevante; (ii) privilegiile de acces sunt limitate la funcționalitatea aprobată a sistemului; (iii) există o separare adecvată a sarcinilor; (iv) privilegiile de acces nu sunt atribuite colectiv (numele de utilizator și parolele să poată fi partajate). Furnizorul se asigură că accesul administrativ la sistemele care stochează sau procesează informațiile DELGAZ GRID este (v) limitat la un număr minim de administratori, (vi) protejat prin procedura de autentificare în doi pași sau în cazul în care autentificarea în doi pași nu este posibilă din punct de vedere tehnic, măsuri de securitate echivalente (de ex. parole generate temporar în sistemele de management). Furnizorul se asigură de asemenea că accesul administrativ este (vii) întotdeauna înregistrat pentru a permite detectarea și investigarea accesului neautorizat și a manipulării neautorizate a informațiilor DELGAZ GRID. (viii) Mai mult decât atât, Furnizorul se asigură că există o procedură oficială în vigoare, care descrie modul în care sunt create, revizuite în mod regulat, modificate, blocate și șterse rolurile, conturile, drepturile de acces și privilegiile privind accesul administrativ.

- 1.8 Rețele și comunicații:** Furnizorul asigură proiectarea rețelelor fizice, wireless și, dacă este cazul, a rețelelor de voce, pentru ca acestea să fie (i) fiabile și rezistente, (ii) să împiedice accesul neautorizat, (iii) să utilizeze conexiuni criptate și (iv) să detecteze traficul suspect. (v) Furnizorul asigură configurarea dispozitivelor de rețea (inclusiv routere, firewall-uri și puncte de acces wireless) pentru a funcționa conform cerințelor și pentru a preveni actualizările neautorizate și incorecte. Furnizorul asigură protejarea sistemelor de comunicații electronice prin (vi) stabilirea politicii de utilizare a acestora, (vii) configurarea setărilor de securitate, (viii) securizarea infrastructurii tehnice de sprijin. (ix) Furnizorul asigură ascunderea numelor computerelor și a rețelelor și a topologiilor față de terți. Furnizorul se asigură că restricționează accesul extern la sistemele și rețelele informatice prin (x) stabilirea zonelor demilitarizate (DMZ) între rețelele nesecurizate și rețelele interne, (xi) rutarea traficului de rețea prin firewall-uri sau firewall-uri proxy, (xii) limitarea metodelor de conectare la minimul necesar, (xiii) acordarea accesului doar la aplicațiile de business autorizate, la sistemele informatice sau la anumite părți ale rețelei.
- 1.9 Managementul Securității Tehnice:** Furnizorul instalează soluții de protecție împotriva programelor malware pe sisteme în care informațiile DELGAZ GRID pot fi expuse la programe malware, inclusiv (i) servere (de exemplu servere de aplicații, servere de baze de date, servere de fișiere, servere de printare, servere web, (ii) tehnică de calcul (de exemplu computere de tip desktop, laptopuri și alte dispozitive mobile) și (iii) echipamente de birou (de exemplu imprimante de rețea, fotocopioare, dispozitive multifuncționale). (iv) Software-ul de protecție împotriva programelor malware trebuie să protejeze împotriva tuturor formelor de malware (de exemplu viruși, viermi, troieni, spyware, rootkit-uri, software-ul botnet, loggers de tip keystroke, ransomware). (v) Software-ul de protecție împotriva malware-ului trebuie distribuit automat și într-un interval de timp definit. Furnizorul se asigură și revizuieste periodic dacă (vi) software-ul de protecție împotriva malware-ului nu a fost dezactivat sau funcționalitatea minimizată, (vii) configurația software-ului de protecție împotriva programelor malware este corectă, (viii) actualizările sunt aplicate corect, într-un interval de timp definit, (ix) scanările sunt efectuate la intervale de timp predeterminate și (x) se furnizează o notificare adecvată a evenimentelor malware identificate.
- 1.10 Dezvoltarea/ achiziționarea de software:** Furnizorul se asigură că software-ul dezvoltat intern sau software-ul achiziționat extern, utilizat pentru procesarea, stocarea sau transmiterea informațiilor DELGAZ GRID, nu este vulnerabil în ceea ce privește "OWASP TOP Ten" și "SANS Top 25 Errors of the Most Dangerous Software".

- 1.11 Scanarea de Vulnerabilități:** Furnizorul se asigură că (i) sistemele accesibile în mod public sunt testate în mod regulat (cel puțin lunar) împotriva vulnerabilităților și a defecțiunilor de configurare prin efectuarea de teste dinamice (teste de penetrare sau scanări de vulnerabilitate). (ii) Toate rezultatele acestor teste relevante pentru DELGAZ GRID sunt partajate cu DELGAZ GRID fără întârziere; (iii) vulnerabilitățile critice vor fi raportate la DELGAZ GRID imediat. (iv) Furnizorul oferă asistență și sprijin pentru auditul patch-urilor de securitate și a managementului vulnerabilităților realizat de DELGAZ GRID. (v) Atenuarea vulnerabilităților de securitate va fi efectuată pe baza nivelului de risc și a intervalelor de timp convenite între părți.
- 1.12 Nivele de patch-uri actualizate:** Furnizorul asigură remedierea vulnerabilităților tehnice prin administrarea unui proces de gestionare a patch-urilor care asigură (i) identificarea și obținerea de patch-uri din surse autorizate, imediat ce acestea sunt disponibile, (ii) decizia când pot fi distribuite patch-urile, (iii) patch-uri de testare pe baza unor criterii cunoscute, (iv) distribuirea patch-urilor în timp util.
- 1.13 Cerințe Minime de Autentificare:** Trebuie aplicat principiul celor mai puține privilegii și necesitatea de a cunoaște și separarea sarcinilor. Mai mult, trebuie aplicat un model de control al accesului bazat pe roluri.
- 1.14 Securizare (Hardening):** Toate sistemele informatice și de rețea trebuie securizate. Aceasta include (i) dezactivarea aplicațiilor, serviciilor, instrumentelor, protocoalelor și interfețelor inutile, (ii) ștergerea sau cel puțin schimbarea numelor de utilizator și a parolilor livrate de furnizori, (iii) activarea opțiunilor de sporire a securității și (iv) prevenirea transferului de informații tehnice către entități externe.
- 1.15 Înregistrarea evenimentelor de securitate:** Pentru a permite detectarea și investigarea accesului neautorizat și a manipulării neautorizate a informațiilor DELGAZ GRID, Furnizorul se asigură că (i) înregistrarea evenimentelor este activată permanent pentru toate sistemele operate de acesta pentru a crea, stoca, procesa sau transmite informații DELGAZ GRID, (ii) sistemele sunt configurate astfel încât să genereze evenimente legate de securitate (inclusiv tipuri de evenimente cum ar fi încercările de conectare reușită și nereușită a utilizatorilor, crearea / modificarea / ștergerea serviciului, crearea / modificarea / ștergerea obiectelor, disfuncționalitatea sistemului, ștergerea conturilor de utilizator) precum și atributele asociate fiecărui eveniment (de exemplu data, ora, ID-ul utilizatorului, numele fișierului și adresa IP), (iii) sursele coerente de date și de timp fiabile asigură ca jurnalele de evenimente utilizează mărci temporale precise (de exemplu: prin utilizarea serverelor NTP), (iv) jurnalele de evenimente de securitate sunt protejate împotriva accesului neautorizat și modificării/suprascrierii accidentale sau intenționate
- 1.16 Managementul Conformității:** Furnizorul se asigură că (i) toate sistemele care creează, stochează, procesează sau transmit informații DELGAZ GRID sunt scanate periodic pentru a respecta "Politicile / Standardele de Securitate proprii ale Furnizorului. (ii) "Politicile / Standardele de Securitate" proprii ale Furnizorilor trebuie mapate și în concordanță cu cerințele menționate în prezenta Anexă. (iii) Rapoarte de conformitate care să dovedească astfel de verificări de conformitate tehnice pentru fiecare activ IT în mediul IT sunt furnizate către DELGAZ GRID la cerere.
- 1.17 Securitatea Resurselor Umane:** Pentru fiecare persoană care acționează în numele furnizorului și căreia i se acordă permisiuni de acces (la nivel local sau de la distanță), informațiile de identificare a persoanei trebuie puse la dispoziția Clientului. Furnizorul asigură o verificare personală a identității entităților umane și că nimeni nu abuzează de

accesul sau permisiunea acordată persoanelor de către Furnizor. În plus, Furnizorul își asumă responsabilitatea pentru orice daune produse datorită accesului neautorizat și / sau utilizării informațiilor DELGAZ GRID. Furnizorul delegă doar personalul care este calificat în mod demonstrabil pentru sarcinile necesare.

- 1.18** Securitatea Lanțului de Aprovizionare: Furnizorul asigură identificarea și gestionarea riscurilor aferente informațiilor pe parcursul fiecărei etape a relațiilor cu furnizorii externi de hardware și software în întregul lanț de aprovizionare prin (i) încorporarea cerințelor de securitate privind informațiile în contracte formale și (ii) obținerea asigurării că acestea sunt îndeplinite. (iii) Furnizorul se asigură că subcontractanții implicați în prelucrarea, stocarea, transmiterea sau eliminarea informațiilor DELGAZ GRID îndeplinesc cel puțin cerințele convenite în prezenta Anexă. (iv) Furnizorul este responsabil pentru asigurarea unei guvernări adecvate a subcontractantului/ subcontractanților, precum și pentru conformitatea controalelor externalizate.

2 Interfețele Procesului de Securitate IT

- 2.1** Ambele părți sunt de acord să comunice și să pună la dispoziție persoane de contact pentru următoarele procese de securitate IT:

- 2.1.1** Managementul Conformității: Pentru a schimba informații cu privire la respectarea cerințelor, a furniza în mod constant rapoarte, astfel cum sunt definite în prezenta Anexă, și a discuta și a conveni asupra acțiunilor de gestionare a neconformităților existente și a riscurilor aferente.
- 2.1.2** Managementul Incidentelor de Securitate IT: Pentru a schimba informații privind incidentele de securitate IT sau evenimentele de securitate IT care ar putea conduce la un incident de securitate IT care afectează sau ar putea afecta mediul IT utilizat pentru stocarea sau procesarea informațiilor Delgaz Grid. "Managementul incidentelor de securitate IT" include, de asemenea, gestionarea solicitărilor de expertiză /emise de către Delgaz Grid.
- 2.1.3** Managementul Riscului: Pentru a schimba informații privind activitățile de gestionare a riscurilor efectuate de Furnizor pentru a asigura identificarea, evaluarea, gestionarea, monitorizarea și menținerea într-o limită acceptabilă, în mod permanent, a riscurilor legate de securitatea informațiilor.
- 2.1.4** Managementul Vulnerabilităților: Pentru a schimba informații privind vulnerabilitățile care afectează sau ar putea afecta mediul IT utilizat pentru stocarea sau procesarea informațiilor Delgaz Grid și pentru a discuta și a conveni asupra acțiunilor de atenuare a vulnerabilităților existente.
- 2.1.5** Managementul Patch-urilor: Pentru a schimba informații privind ferestrele de mentenanță agreate și distribuirea de patch-uri.

- 2.1.6 Managementul Identității și Accesului: Pentru a schimba informații privind subiectele legate de Managementul Identității și Accesului.
 - 2.1.7 Confidențialitatea Datelor: Să facă schimb de informații cu privire la activitățile și incidentele legate de confidențialitatea datelor.
- 2.2 Ambele părți sunt de acord să colaboreze și să facă schimb de informații în cadrul fiecăruia dintre procesele de securitate menționate mai sus. Părțile vor conveni asupra unor mijloace tehnice privind schimbul de informații, precum și a indicatorilor-cheie de performanță (KPI) în vederea asigurării conformității cu procedurile de securitate convenite.
- 2.3 Ambele părți sunt de acord că persoanele de contact desemnate pentru procesele de securitate menționate mai sus există și pot fi înlocuite. În cazul înlocuirii, partea care înlocuiește o persoană de contact desemnată va informa prompt cealaltă parte.

Persoana de contact Delgaz Grid

Securitatea Informației

Nume și prenume: Truță Mihai

Adresă de e-mail: it_security_romania@eon.com

Persoană de contact Prestator

Nume și prenume:

Telefon:

Adresă de e-mail: