Aprobat prin decizia Consiliului de administrație
al Întreprinderii Municipale Parcul „Dendrariu”,
provesul-verbal nr. 3 din 07.02. 2023

POITICA

de securitate cibernetică a Întreprinderii Municipale Parcul „Dendrariu”

I. Scopul, obiectivele și domeniul de activitate

1. Politica internă privind securitatea cibernetică a întreprinderii are ca scop asigurarea integrității, confidențialității și disponibilității informației, precum și asigurarea colectării, procesării, stocării și accesării în siguranță a datelor, inclusiv a datelor de interes public.

2. Politica internă privind securitatea cibernetică a întreprinderii se aplică în cadrul întreprinderii față de:

1) echipamentele (hardware) și produsele de program (software) existente în cadrul întreprinderii;

2) sistemele informatice, resursele și sistemele informaționale existente în întreprinderii (în continuare – sisteme), precum și cele aflate la etapa de elaborare, testare și implementare.

3. Realizarea scopului Politicii interne privind securitatea cibernetică a întreprinderii, presupune atingerea următoarelor obiective:

1) Respectarea/ punerea în aplicare a prevederilor cadrului legislativ-normativ național și internațional, inclusiv a standardelor, în domeniul securității cibernetice;

2) Implementarea măsurilor de securitate cibernetică în scopul respectării Cerințelor minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201 din 28.03.2017;

3) Implementarea măsurilor organizaționale direcționate spre reglementarea internă a procedurilor de securitate cibernetică;

4) Prevenirea accesului neautorizat la sistemele întreprinderii;

5) Garantarea funcționării neîntrerupte și în siguranță a sistemelor întreprinderii;

6) Asigurarea intervenției prompte, eficiente și sistematice la incidentele de securitate cibernetică;

7) Sporirea calificării angajaților întreprinderii în domeniul securității cibernetice;

8) Realizarea măsurilor de evaluare și management a riscurilor cibernetice ale întreprinderii, sporirea nivelului de protecție a sistemelor, hardware și software ale întreprinderii.

4. Scopul securității cibernetice este de a proteja sistemele, echipamentele și produsele de program ale întreprinderii, de a asigura continuitatea activității și de a minimiza daunele aduse întreprinderii prin prevenirea și minimizarea impactului incidentelor de securitate.

II. Principiile de organizare internă a managementului de securitate cibernetică

5. Sistemul de management al securității cibernetice a întreprinderii are la bază următoarele principii:

1) *confidențialitatea* - asigurarea faptului că informația este accesibilă doar persoanelor autorizate. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prinprocedurile de acces la sistemele informaționale;

2) *integritatea* - păstrarea acurateței și completitudinii informației, precum și a metodelorde procesare;

3) *disponibilitatea* - asigurarea faptului că utilizatorii autorizați au acces la informație și la resursele asociate atunci când este necesar. Diverse software necesită nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a sistemelor informaționale:

4) *nonrepudierea* - asigurarea faptului că, după emiterea/ recepționarea unei informații într-un sistem de comunicații securizat, expeditorul/ destinatarul nu poate nega, în mod fals, că a expediat/ primit informațiile în cauză.

III. Analiza situației și vulnerabilităților

6. Pentru implementarea politicii interne privind securitatea cibernetică, întreprinderea va efectua un audit intern de securitate cibernetică, care cuprinde următoarele chestiuni:

1) Evaluarea vulnerabilităților/ riscurilor: se identifică amenințările asupra resurselor și amenințările care trebuie eliminate și/ sau care pot fi tolerate, se evaluează vulnerabilitatea față de aceste amenințări și probabilitatea de producere a lor și se estimează impactul potențial; ierarhizarea riscurilor;

2) Identificarea sistemelor, echipamentelor și produselor de program care trebuie protejate și la ce nivel;

3) Mijloacele, prin care este implementată securitatea cibernetică.

IV. Declarația managementului întreprinderii de susținere a scopului și principiilor politicii interne privind securitatea cibernetică a întreprinderii

7. Conducerea întreprinderii își asumă responsabilitatea pentru organizarea și gestionarea activității privind menținerea și îmbunătățirea sistemului de management al securității cibernetice.

V. Respectarea și implementarea politicii interne privind securitatea cibernetică a întreprinderii

8. Persoana responsabilă de punerea în aplicare a sistemului de management al securității cibernetice în întreprinderii, întreprinde toate măsurile necesare pentru protecția sistemelor, echipamentelor și produselor de program

împotriva amenințărilor interne sau externe, deliberate sau accidentale, pentru a asigura că:

1) informațiile, serviciile și sistemele sunt protejate împotriva accesului neautorizat;

2) confidențialitatea informațiilor este păstrată;

3) integritatea informațiilor, serviciilor și a sistemelor este păstrată;

4) disponibilitatea informațiilor, serviciilor și sistemelor este asigurată atunci când procesele activității o cer;

5) cerințele și obiectivele organizaționale sunt îndeplinite;

6) cerințele legislative și de reglementare sunt îndeplinite.

9. Prevederile Politicii interne privind securitatea cibernetică a întreprinderii, a Regulamentelor și procedurilor se respectă și se aplică nediscriminatoriu de către toți angajații întreprinderii cărora li s-a autorizat accesul la sistemele, echipamente și produse de program, precum și altor persoane fizice și juridice (consultanți, experți, stagiari, auditori externi, inspectori etc.).

10. Fiecare utilizator autorizat al sistemelor, echipamentelor și produselor de program a întreprinderii poartă răspundere personală pentru aplicarea întocmai în activitatea sa a regulamentelor și procedurilor de securitate cibernetică în vigoare, elaborate și aprobate, conform standardelor internaționale, legislației naționale speciale și a reglementărilor interne de funcționare. De asemenea, orice utilizator autorizat al sistemelor, echipamentelor și produselor de program are obligația raportării oricărui incident de securitate.

11. Nerespectarea Politicii interne privind securitatea cibernetică a întreprinderii atrage după sine aplicarea unor măsuri disciplinare, precum și revizuirea drepturilor de acces la informație.

12. Politica internă privind securitatea cibernetică a întreprinderii poate fi revizuită la dispoziția managementului în vederea actualizării și adaptării la noile condiții și cerințe.

Director Î.M. Parcul „Dendrariu” **Ion Uzun**