

Securitate

Modulul Securitate din Mago.Net vă permite asocierea la profile a utilizatorilor, autorizând astfel accesul doar la datele de care au nevoie și pentru care sunt responsabili.

Modulul Securitate din Mago.Net vă permite asocierea la profile a utilizatorilor, autorizând astfel accesul doar la datele de care au nevoie și pentru care sunt responsabili.

Nivelul de acces se aplică și la accesul prin Internet.

Gestionarea accesului este complet integrat în Mago.Net și are la bază Serviciile Web.

Atunci când un utilizator se autentifică în program de la o stație de lucru, server-ul verifică personalizările acestuia, astfel încât doar funcțiile la care are acces vor fi disponibile.

Administratorul de sistem poate stabili ce funcții și câmpuri pot fi accesate de fiecare utilizator sau rol și dacă pot fi doar citite sau și editabile. Un utilizator poate fi asociat la mai multe roluri, având astfel un sistem de permisiuni mai flexibil.

Există și un set de proceduri automate ce ajută Administratorul de Sistem să aplice „în masă” politicile de securitate, politici ce pot fi modificate mai târziu pentru fiecare utilizator unde este cazul.

Sistemul de autentificare în program poate fi cel folosit de Windows, cel folosit de Sql Server sau o combinație între cele două.

Această flexibilitate este utilă atunci

când, spre exemplu, doriți să atribuiți fiecărui utilizator un cont de acces la baza de date diferit de cel de acces în Mago.Net. Pentru acești utilizatori, baza de date este complet inaccesibilă cu alte instrumente în afară de Mago.Net.

Utilizatorul poate folosi același cont și parolă pentru a accesa sistemul de la orice stație de lucru din LAN sau din internet, spre exemplu, prin EasyLook. Drepturile lui de acces se vor păstra, indiferent de metoda de acces.

Utilizarea tehnologiei Servicii Web are un mai bun efect în rețele complexe multi-protocol sau în rețelele heterogene ce nu au configurații standard. Performanțele aplicației au fost îmbunătățite, rezultând o creștere semnificativă a vitezei de procesare.

Modulul Securitate din Mago.Net Professional Edition satisface nevoile de securitate și privacy pentru administrarea datelor într-un sistem informatic de afaceri, astfel încât companiile să își poată îndeplini toate obligațiile prevăzute de legislația în vigoare cu privire la privacy.

Este recomandat pentru instalări cu posturi de lucru numeroase și pentru acele companii care au nevoie să își protejeze date „sensibile”, unde fiecare utilizator trebuie asociat unui rol în concordanță cu îndatoririle sale.

Cu ajutorul modulului Securitate, se

poate controla accesul la funcțiile aplicației și la date prin definirea de profile de securitate personalizabile. Se pot defini departamente, se pot atribui privilegii speciale și se pot apoi asocia utilizatorii din acele departamente.

Privilegii sau restricții adiționale se pot asocia mai târziu utilizatorilor individuali.

Spre exemplu, în cazul departamentului „Personal administrativ”, se pot seta profilele „senior” și „junior” în concordanță cu nivelul de complexitate și confidențialitate a datelor la care ei trebuie să aibă acces.

Pentru diferite „obiecte” (tab-uri, grile, coloane, etc.) ce includ date, se pot seta restricții suplimentare pentru a crește nivelul de confidențialitate acolo unde este necesar. Astfel, se poate acorda sau interzice accesul la date și chiar la editarea, adăugarea sau ștergerea lor.

Există multe aplicații potențiale pentru acest modul: este foarte importantă protejarea integrității datelor, mai ales a celor importante, cum ar fi situații financiare, jurnale de TVA și înregistrări contabile, reducând astfel riscul de erori datorită accesului sau modificărilor neautorizate.

Un profil „Contabil Junior” poate avea dreptul să introducă și să salveze facturi, documente de vânzări și achiziții și informații despre clienți și furnizori, în timp ce un „Contabil Junior” va

introduce conturile pe care se vor duce aceste documente și va avea acces la date mai „sensibile” despre afacere (spre exemplu, refuzuri la plată, împrumuturi, condiții de plată, litigii, etc.).

Accesul la funcțiile de introducere a datelor contabile poate fi acordat unui „senior” sau unui specialist extern (de obicei un contabil) cu o mai mare experiență și responsabilitate, deoarece ei pot vedea situații financiare și închiderile contabile.

O altă aplicabilitate este legătura dintre Vânzări și Logistică. Și aici, păstrarea confidențialității poate cere ca Notele de livrare să fie emise fără ca persoana care se ocupă de vânzări să vadă anumite date, și mai ales comisioanele sale.

Se poate autoriza ca Directorul Financiar să poată stabili centrele de cost, ca și conturile corespondente pentru facturile primite. Drepturi de acces similare pot fi stabilite și pentru zonele de Comenzi și Achiziții. Astfel, se pot stabili personalizări pentru plăți și proteja modificarea lor. Se pot proteja de asemenea și modelele contabile și jurnalele de TVA pentru a nu putea fi editate, astfel încât departamentul de vânzări să nu poată modifica termenele de plată sau listele de prețuri.

Se poate stabili ce se vede și/sau ce se poate edita practic în orice pagină, tabel sau chiar într- o coloană dintr-

un tabel.

Flexibilitatea acestei aplicații este evidentă, unul din avantajele fiind posibilitatea de a accesa baza de date fără probleme și cu cât mai puține resurse implicate.

Acest rezultat se obține datorită timpului ce nu se mai pierde la corectarea erorilor datorate introducerii greșite de date de către personalul nepregătit sau neautorizat.

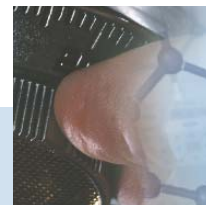
Nu trebuie să mai menționăm crearea unui sistem eficient și ușor de implementat pentru gestionarea confidențialității datelor importante pentru afacerea dumneavoastră.

În Master-ul pentru Articole se poate autoriza personalul din depozit să adauge articole noi, dar să nu poată modifica listele de prețuri, care pot sau nu să fie vizibile.

Drepturile de acces se pot stabili pentru o persoană sau pentru o „funcție”, iar la o „funcție” pot fi asociate mai multe persoane.

Spre exemplu, la funcția „operator depozit” pot fi asociate mai multe persoane, cum ar fi Ionut Popescu și George Ionescu. Vice versa, o persoană poate fi asociată la mai multe funcții, cum ar fi „Manager vânzări”, „Responsabil buget”, „Agent”, etc.

După cum vedeți, administrarea acestor funcții este foarte ușoară, având la dispoziție o mare flexibilitate pentru atribuirea de drepturi de acces și pen-



Modulul Securitate din Mago.Net vă permite asocierea la profile a utilizatorilor, autorizând astfel accesul doar la datele de care au nevoie și pentru care sunt responsabili.

tru asocierea angajaților la aceste funcții.

În departamentul Contabilitate poate fi nevoie să existe o funcție „Contabil Junior” care să poată introduce înregistrări contabile și informații despre clienți sau furnizori, în timp ce „Contabilul Senior” va stabili ce conturi se vor folosi pentru aceste înregistrări și va avea acces la date mai „sensibile” despre afacere (spre exemplu, refuzuri la plată, împrumuturi, condiții de plată, litigii, etc.)

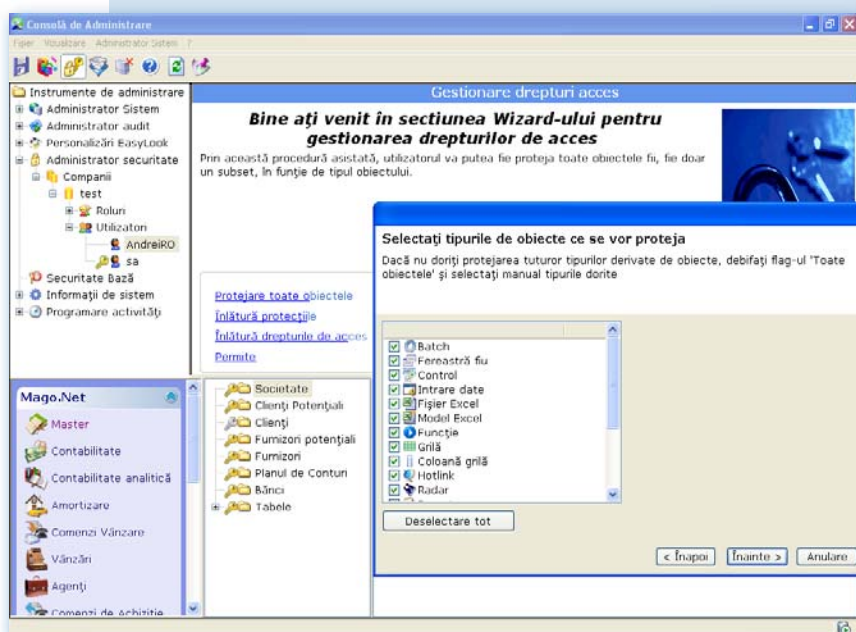
În acest fel, „juniorul” poate doar să introducă date, cum ar fi achizițiile, iar „seniorul” sau un specialist extern (de obicei un Contabil) va introduce conturile corespondente și va asocia

diverse conturi de venituri și cheltuieli.

Acest modul este util pentru protejarea declarațiilor fiscale, reducând riscul apariției de erori în calculul impozitului pe profit, evitând astfel plata de penalități sau cheltuieli suplimentare.

Evident, situațiile financiare, ca și jurnalele de TVA și înregistrările contabile pot fi protejate.

Pentru Lista de Materiale, drepturile de acces pot fi date doar departamentului Logistic pentru definirea compoziției produsului (rețetei), astfel încât să nu fie modificate de personal neautorizat.



www.microarea.it