

# 360° Προστασία και ασφάλεια των δεδομένων

## Βέλτιστη διαχείριση των δεδομένων με κανόνες & διαφάνεια

Η ασφάλεια και προστασία των δεδομένων είναι το βασικότερο δομικό στοιχείο των πληροφοριακών συστημάτων. Καθώς η πολυπλοκότητα αυξάνεται και η πρόσβαση στα δεδομένα γίνεται από πολλαπλά κανάλια, συστήματα και συσκευές, το Entersoft Business Suite είναι εξοπλισμένο με πολλαπλά επίπεδα ελέγχου πρόσβασης στα δεδομένα, τα οποία επεκτείνει και προσαρμόζει διαρκώς στις τεχνολογικές και θεσμικές εξελίξεις, μέσω ενός πανίσχυρου framework που χρησιμοποιείται από όλη τη γκάμα των εφαρμογών από όπου κι αν αυτές εκτελούνται (On premises, On cloud, μέσω browsers ή mobile devices & tablets).



### Διαχείριση στοιχείων ασφάλειας

#### Πολιτική κωδικών πρόσβασης

Απλός-ισχυρός κωδικός, παραμετρικοί κανόνες πολυπλοκότητας κωδικών, συχνότητα αλλαγής-διάρκεια κωδικού (σε ημέρες), άμεση αλλαγή στην επόμενη είσοδο στο σύστημα. Το Entersoft framework χρησιμοποιεί τον αλγόριθμο DES για κρυπτογράφηση των κωδικών πρόσβασης.

#### Κανάλι πρόσβασης

Προσδιορισμός καναλιού από το οποίο μπορεί ένας χρήστης να αποκλειστεί π.χ. από το internet ή άλλο subnet ή από συγκεκριμένες IP.

#### Πιστοποίηση μέσω LDAP

Πιστοποίηση μέσω δικτύου (Lightweight Directory Access Protocol) για εκμετάλλευση από τον domain server.

#### Two factor authentication

Η απαίτηση για επιβεβαίωση δύο βημάτων για πρόσβαση σε Desktop εφαρμογές ή και WebApi ή και e-Commerce κ.λπ. μπορεί να ενεργοποιηθεί ανά χρήστη. Μπορεί μάλιστα να οριστεί ότι για τον ίδιο χρήστη ενεργοποιείται TFA μόνο για τα Web Apps κι όχι τις Desktop εφαρμογές. Για τη διαμόρφωση του TFA σε κινητά, χρησιμοποιείται είτε ο Microsoft Authenticator είτε ο Google Authenticator.

#### Απενεργοποίηση λογαριασμού χρήστη

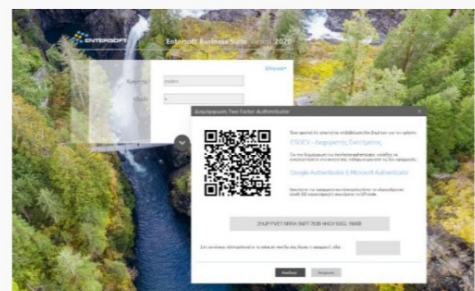
Μετά από επαναλαμβανόμενες αποτυχημένες προσπάθειες εισόδου, μπορεί να απενεργοποιείται ο χρήστης, προς επανέλεγχο.

#### Καθορισμός χρήστη ως "read-only"

Με μία μόνο κίνηση, χωρίς πρόσθετες διαδικασίες προσδιορισμού δικαιωμάτων πρόσβασης, μπορεί να προσδιοριστεί πως ο χρήστης δεν μπορεί να αποθηκεύει, παρά μόνο να προβάλλει πληροφορίες.

#### Μενού χρήστη

Ένας εύκολος τρόπος περιορισμού των χρηστών σε συγκεκριμένες λειτουργίες που τους αφορούν (κυρίως για λόγους απλότητας και κατανόησης και όχι διότι υπάρχει εξασφάλιση του αποκλεισμού τους από όλα τα άλλα) είναι και ο καθορισμός συγκεκριμένου μενού ανά χρήστη, αντί του πλούσιου μενού των εφαρμογών.



### Πρόνομα πρόσβασης



## Πρόσβαση στη λειτουργικότητα

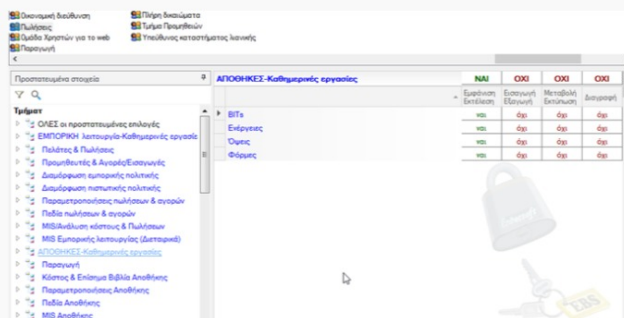
Το σύνολο των οντοτήτων, των λειτουργιών, των προβολών, των εκτυπώσεων, των dashboards, των μαζικών διαδικασιών και των πεδίων είναι διαθέσιμα για απονομή ή αποκλεισμό δικαιωμάτων πρόσβασης σε “ρόλους χρηστών”. Αν κάποιος χρήστης έχει πολλούς “ρόλους”, τα δικαιώματα πρόσβασης στο σύστημα “συγκωνεύονται” (αθροίζονται). Αν δεν αποδοθεί δικαίωμα πρόσβασης σε κάποια λειτουργικότητα, αυτόματα ερμηνεύεται ως “αποκλεισμός”.

Η απονομή των δικαιωμάτων μπορεί να γίνει σε ολόκληρες περιοχές λειτουργικότητας με μαζικό τρόπο είτε σε επίπεδο λεπτομέρειας (το οποίο υπερিশύει), μέχρι και σε επίπεδο πεδίου.

Υπάρχει μάλιστα η δυνατότητα απόκρυψης περιεχομένου “ευαίσθητων” πεδίων (data masking) σε επίπεδο user interface (π.χ. Όνομα ως \*\*\*\*, τηλέφωνο ως 210\*\*\*\*50 κ.ο.κ.), που αποτελεί έναν από τους αποτελεσματικότερους μηχανισμούς ελέγχου πρόσβασης σε προσωπικά δεδομένα. Έτσι, κάποιοι χρήστες μπορούν να εισάγουν δεδομένα, αλλά μετά την εισαγωγή να μην μπορούν να τα δουν, (σε συνδυασμό με τον αποκλεισμό τους από τη δυνατότητα μεταβολής).

Τα δικαιώματα πρόσβασης είναι διεταιρικά, ισχύουν δηλαδή για όλες τις εταιρείες στις οποίες έχει πρόσβαση κάθε χρήστης.

Τα δικαιώματα μπορούν να προσδιοριστούν για κάθε επί μέρους λειτουργικότητα, αναλόγως της περιοχής που αναφέρονται (εισαγωγή, τροποποίηση, εμφάνιση, διαγραφή, εκτύπωση, εκτέλεση – αν πρόκειται για προβολή/query, εξαγωγή στοιχείων-cory στο clipboard κ.λπ.)



## Πρόσβαση σε συγκεκριμένες οντότητες

Ειδικά στις σειρές παραστατικών, τα δικαιώματα απονέμονται ξεχωριστά ανά σειρά (ή και μαζικά με ειδικές διαδικασίες) και αφορούν και πρόσθετες δυνατότητες όπως τον αποκλεισμό επέμβασης σε τιμές/εκπτώσεις, τον αποκλεισμό διαγραφής γραμμής ή αλλαγής είδους, την εισαγωγή με πληκτρολόγηση (μπορεί να επιτρέπεται ΜΟΝΟ μέσω μετάβασης από προηγούμενο στάδιο της διαδικασίας δηλαδή) κ.λπ.

Τα παραστατικά που λογιστικοποιούνται περιέχουν μεν στοιχεία που αφορούν τη Λογιστική, αλλά και πληθώρα πληροφοριακών ή διοικητικών στοιχείων που δεν αφορούν τη Λογιστική. Για το λόγο αυτό, το Entersoft Business Suite παρέχει σύστημα υπέρβασης των ελέγχων λογιστικοποίησης για συγκεκριμένους ρόλους χρηστών, για διάφορες κλάσεις δεδομένων όπως π.χ. στοιχεία διαμόρφωσης cash flow, εταιρικές διαστάσεις, στοιχεία πωλητών-προμηθειών κ.λπ., μέσω ενός end-user-interface. Παράλληλα, μπορεί κανείς να ορίσει για συγκεκριμένες συναλλαγές, για συγκεκριμένες ομάδες χρηστών, υπό συγκεκριμένες συνθήκες, ένα σύνολο πρόσθετων απαγορεύσεων (από εκείνες που το σύστημα εκτελεί σε “επίσημες” εγγραφές) π.χ. απαγόρευση μεταβολής του σταδίου εξέλιξης, των οριζόμενων πεδίων κ.λπ.

Ειδική μνεία υπάρχει και για διάφορες οντότητες όπου η πρόσβαση είναι χρήσιμο να είναι ανά περίπτωση και όχι μαζικός αποκλεισμός ή δικαίωμα πρόσβασης όπως:

- οι ενέργειες & δράσεις στελεχών τμημάτων πωλήσεων και εξυπηρέτησης πελατών (ραντεβού, σεμινάρια, επισκέψεις, αιτήματα, επιλύσεις, παράπονα κ.ο.κ.)
- τα φύλλα προϋπολογισμού, που προστατεύονται από ένα εκτενές σύστημα ρόλων (συντάκτη, υπεύθυνου προέγκρισης, έγκρισης κ.λπ.) με όρια ημ/νιών για μεταβολές & οριστικοποίηση, με ελέγχους ανάλογα με την “κατάσταση” κ.λπ.

## Προστασία στο customization επίπεδο

Σε επίπεδο οντοτήτων, φορμών, πεδίων, εκτυπωτικών, παραστατικών κ.λπ. που προστέθηκαν σε επίπεδο υλοποίησης, ολόκληρο το σύστημα δικαιωμάτων είναι διαθέσιμο και λειτουργεί ακριβώς σαν να πρόκειται για το επίπεδο τυποποίησης που δίνεται έτοιμο με το προϊόν. Σε επίπεδο business rules & processes που ορίζονται από τον υπεύθυνο υλοποίησης, χρειάζεται να ενσωματωθεί ειδική πρόβλεψη για την ομάδα χρηστών που θα έχει πρόσβαση στις σχετικές διαδικασίες, ΑΝ χρειάζεται, αφού πολλές φορές, η πρόσβαση εξασφαλίζεται από την τοποθέτηση της δυνατότητας ή της διαδικασίας σε οθόνες ή λίστες ή οντότητες όπου ΗΔΗ έχουν προσδιοριστεί δικαιώματα.

## Πρόσβαση μέσω Web API με χρονική προθεσμία

Κάθε σύνδεση με τον Application Server μέσω του Entersoft Web API χρησιμοποιεί διακριτικό ασφαλούς πρόσβασης που έχει διάρκεια μερικά λεπτά, οπότε και ακυρώνεται, ενώ σε οποιαδήποτε επόμενη κλήση ανανεώνεται με τον ίδιο κανόνα. Η διάρκεια ποικίλλει ανάλογα με τη φύση της εφαρμογής (Entersoft Analyzer, Request For Approval, Integration service όπως ο Entersoft eCom Connector ή ο Connector για το Microsoft Power BI κ.λπ.

## Ασφάλεια σύνδεσης στο Entersoft Cloud

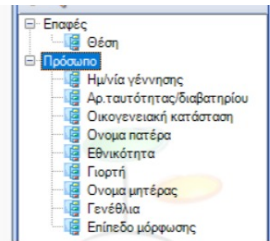
Η πλήρης λίστα των διακομιστών και των services που αποτελούν μέρος του Entersoft Web API και των Entersoft Web εφαρμογών διασφαλίζεται μέσω Green Level Certificates που εκδίδονται από παγκόσμιους αξιόπιστους οργανισμούς και υποστηρίζονται από όλους τους browsers, σε όλες τις πλατφόρμες και συσκευές.

## Προστασία δεδομένων στο Entersoft Cloud

Η αρχιτεκτονική του Entersoft Web API που συνδέει τον Entersoft Application Server (EAS) με όλες τις εφαρμογές του Entersoft Cloud Store δεν αποθηκεύει ποτέ δεδομένα που μεταφέρονται μεταξύ των clients, του Web API και του EAS.



- Διαδικασία τεκμηρίωσης της πολιτικής GDPR
- Διαδικασία γνωστοποίησης του σκοπού χρήσης και επεξεργασίας προσωπικών δεδομένων
- Διαδικασία αποστολής καμπάνιας ενημέρωσης και λήψη άδειας χρήσης προσωπικών δεδομένων
- Διαδικασίες αποδοχής, αλλαγής ή κατάργησης τήρησης (anonymization) προσωπικών δεδομένων
- Σύστημα προστασίας των δεδομένων από μη εξουσιοδοτημένους χρήστες (Role Based Security)
- Σύστημα ασφάλειας των δεδομένων σε επίπεδο πεδίου ώστε να μπορεί να γίνει ρύθμιση της αναγνωσιμότητας των "ευαίσθητων" πεδίων μόνο από ρόλους σχετικούς με τα scores που έχουν οριστεί
- Ειδική κλάση πεδίων για τον συγκεκριμένο σκοπό (GDPR), ώστε να αναγνωρίζονται, να προστατεύονται και να ελέγχονται μαζικά, βάσει του σκοπού επεξεργασίας (Field Set Security Grouping - FSSG)
- Ιστορικότητα αλλαγών πεδίων, καθώς και ιστορικότητα εξαγωγής πληροφοριών (exports, print reports, copy to clipboard κλπ.) για εύκολο εντοπισμό πιθανών διαρροών
- Δυνατότητα κρυπτογράφησης (πεδίων, πινάκων) της Βάσης Δεδομένων - διαθέσιμη σε MS SQL Server 2016
- Δυνατότητα απόκρυψης περιεχομένου "ευαίσθητων" πεδίων σε επίπεδο user interface (πχ. Όνομα ως \*\*\*\*, τηλέφωνο ως 210\*\*\*\*50 κ.ο.κ.
- Σε πολυεθνικές εγκαταστάσεις, δυνατότητα απόκρυψης στοιχείων προσωπικών που δεν αφορούν μια εταιρεία (σε Β.Δ. με κοινό κατάλογο προσωπών), ειδικά για εταιρείες του ομίλου εκτός ΕΕ (άρα αντικείμενο GDPR)



## Διαδικασίες διερεύνησης & ελέγχου

Το σύστημα καταγράφει και τεκμηριώνει

- Εισαγωγή, Διαγραφή, Τροποποίηση σε οντότητες και πεδία
- Εκτέλεση διαδικασιών
- Εκτέλεση όψεων & αναφορών κάθε είδους
- Sign-in / Sign-out χρηστών
- Αναβαθμίσεις εκδόσεων

## Ιστορικό αλλαγών

Ειδικά όσον αφορά τα πεδία, το σύστημα προβλέπει καταγραφή ιστορικότητας αλλαγών (χρήστης, ημ/νία, προηγούμενη τιμή) στα συνήθη "ευαίσθητα" πεδία, αλλά μπορεί κανείς να προσθέσει οποιοδήποτε άλλο πεδίο (δυνατότητα απαραίτητη άλλωστε για την περίπτωση που προστεθούν πεδία και πίνακες σε επίπεδο υλοποίησης - customization). Η πρόσβαση στην πληροφορία αυτή είναι έτοιμη μέσα στις οθόνες διαχείρισης οντοτήτων (για έλεγχο συγκεκριμένης οντότητας), αλλά και σε ειδικό μαζικό έλεγχο με κριτήρια στοχευμένα για να βοηθήσουν τον εντοπισμό προβλημάτων.

## Μηνύματα κατά την εκτέλεση διαδικασιών

Κάποιες (χρονοβόρες) διαδικασίες εξάγουν πληροφορίες κατά την εκτέλεσή τους, για το χρόνο, τα αποτελέσματα, το τερματικό κ.λπ. για αξιολόγηση από το τμήμα IT. Τέτοιες είναι η Αποτίμηση αποθεμάτων, τα Κλεισίματα, οι διάφορες εργασίες επαναυπολογισμού κ.ο.κ.

## Ιστορικό συμβάντων

Το σύστημα τηρεί αναλυτικό ιστορικό εκτέλεσης μιας μεγάλης γκάμας "γεγονότων" όπως η είσοδος-έξοδος χρήστη, διαγραφές εγγραφών, εγκρίσεις υπερβάσεων πιστώσεων, λήψη backup, επανεκκίνηση server, αναβαθμίσεις έκδοσης S/W, εργασίες επαναυπολογισμού, λήψη επίσημων εκτυπώσεων κ.λπ., για τα οποία παρέχει όλη την απαραίτητη πληροφορία για να διερευνηθούν πιθανά προβλήματα.



Χρήστ.	Ημερ.	Ώρα	Κωδικός Συστ.	Επερα.	Περιγραφή Συναθροισμ.	Στοιχείο Λειτουργ.
KAR	21/06	13:56	ADDCS-FRR	Αδίκ.	No access or not allowed to access directory (C:\PROGRAM FILES (32BIT	KAR-MO215848-KAR-MO26254-707553-8bde
KAR	21/06	13:56	ADDCS-FRR	Αδίκ.	No access or not allowed to access directory (C:\PROGRAM FILES (32BIT	KAR-MO215848-KAR-MO26254-707553-8bde
KAR	21/06	13:56	ESLOGOUT	Περποραία	Έξοδος χρήστη από την εφαρμογή	ES-ENTERSOFT\Fike\01540023\de1ea71c-65
KAR	21/06	13:56	ESLOGIN	Περποραία	Είσοδος χρήστη στην εφαρμογή	ES-ENTERSOFT\Fike\01540023\de1ea71c-65
KAR	21/06	13:56	ESLOGOUT	Περποραία	Έξοδος χρήστη από την εφαρμογή	ES-ENTERSOFT\Fike\01540023\de1ea71c-65
KAR	21/06	13:56	ESLOGIN	Περποραία	Είσοδος χρήστη στην εφαρμογή	ES-ENTERSOFT\Fike\01540023\de1ea71c-65
KAR	21/06	13:56	ADDCS-FRR	Αδίκ.	No access or not allowed to access directory (C:\PROGRAM FILES (32BIT	KAR-MO215848-KAR-MO2625552075-0227
KAR	21/06	13:56	ADDCS-FRR	Αδίκ.	No access or not allowed to access directory (C:\PROGRAM FILES (32BIT	KAR-MO215848-KAR-MO2625552075-0227

## Audit trail των εφαρμογών στο Entersoft Cloud

- Κάθε σύνδεση σε μια εφαρμογή με συνδρομή στο Entersoft Cloud κρυπτογραφείται, αρχειοθετείται και αποθηκεύεται για μελλοντικό έλεγχο από τον διαχειριστή.
- Για κυλιόμενη περίοδο 90 ημερών, το Entersoft Cloud Store διατηρεί λεπτομερείς πληροφορίες σχετικά με τη χρήση, τα σφάλματα και την κατανάλωση quota, εάν υπάρχουν.

## FAQ

**Πώς επιβάλλεται ο έλεγχος ταυτότητας API και η διαχείριση των credentials, σε περίπτωση που ένα API χρησιμοποιείται χωρίς πύλη API Mulesoft;**

Το Entersoft Web API, υποστηρίζει πλήρως την έννοια των Application Keys, Developer Keys, Security Schemes, Security Policies, System Constraints. Παρέχει όλα τα μέσα σε έναν Πελάτη / Συνδρομητή για τη διαχείριση, παρακολούθηση, καταγραφή, ειδοποίηση του χρόνου εκτέλεσης του Entersoft Web API στο πλαίσιο οποιασδήποτε εφαρμογής που χρησιμοποιεί το Entersoft Web API για Entersoft και Custom εφαρμογές. Η παροχή του Entersoft Web API μέσω ενός συστήματος διαχείρισης πύλης API όπως το Mulesoft ή το Microsoft κ.λπ., θα πρέπει να θεωρηθεί ως επί πληρωμή Custom Add-on στα πλαίσια ενός έργου.

**Πώς παρακολουθούνται συνεχώς τα αρχεία καταγραφής συμβάντων ασφαλείας (security event logs) σε περίπτωση που το σύστημα SIEM δεν χρησιμοποιείται;**

Τα αρχεία καταγραφής ασφαλείας (security logs) δημιουργούνται από τα διάφορα υποσυστήματα και λειτουργικά επίπεδα της αρχιτεκτονικής της εφαρμογής Entersoft και μεταφέρονται συνεχώς στο Entersoft Realtime Monitoring σύστημα που εκτελείται στο Microsoft Azure.

**Ποιος είναι ο μηχανισμός αυθεντικοποίησης για Mobile apps;**

Ανεξάρτητα από τη Λύση MDM που έχει παράσχει και εφαρμοίσει ο Πελάτης, για οποιαδήποτε συσκευή μπορεί να επιτραπεί η πρόσβαση σε έναν «Χρήστη» στο Entersoft Mobile Cross Application που εκτελείται στη Συσκευή, η συσκευή θα πρέπει πρώτα να εγγραφεί στο Σύστημα Back-End της Entersoft και ο χρήστης πρέπει να εκχωρηθεί σε αυτήν τη συσκευή. Επιπλέον, ο Χρήστης θα πρέπει να έχει δικαίωμα πρόσβασης στην κινητή συσκευή. Στη συνέχεια, το User ID/ Password, της αυθεντικοποίησης ενός χρήστη, θα έχει τεθεί σε ισχύ.

**Τα Mobile apps κρυπτογραφούν τα δεδομένα στη συσκευή;**

Η εφαρμογή Entersoft Mobile Merchandising Cross-Platform, αποθηκεύει τα δεδομένα που ορίζονται από τη διαμόρφωση Back-End για να είναι διαθέσιμα offline για τον συγκεκριμένο Χρήστη / Ομάδα / Συσκευή σε μια βάση δεδομένων SQLite που είναι αποθηκευμένη στο sandbox της εφαρμογής που προστατεύεται και κρυπτογραφείται από το Λειτουργικό Σύστημα (Android OD, Apple iOS, Windows UWP). Περαιτέρω κρυπτογράφηση στη βάση δεδομένων SQLite μπορεί να εφαρμοστεί όποτε αυτή η επιλογή είναι διαθέσιμη από την υποκείμενη έκδοση του λειτουργικού συστήματος.

**Πώς μπορούν να διαχειριστούν τα mobile apps από το MDM / MAM σύστημα της εταιρείας;**

Τα Entersoft CRM και Entersoft Mobile SFA προσφέρουν ένα βασικό υποσύστημα MDM που παρέχει τις θεμελιώδεις λειτουργίες για τη Διαχείριση συσκευών, δηλαδή τη σύζευξη της συσκευής με έναν χρήστη και μια εφαρμογή Entersoft, ενεργοποίηση / απενεργοποίηση της συσκευής, συσχέτιση / αποσυσχέτιση ενός χρήστη σε μια συσκευή και ενός Entersoft app στη συσκευή. Επιπλέον, το Entersoft core MDM Subsystem παρέχει λειτουργίες σε σχέση με τις Entersoft Mobile Apps όπως: Κλείδωμα συσκευής, Απαγόρευση συγχρονισμού δεδομένων σε μία ή και στις δύο κατευθύνσεις, Καταχώριση της τελευταίας γνωστής τοποθεσίας της Συσκευής (υποθέτοντας ότι ο Χρήστης έχει αποδεχτεί και ενεργοποιήσει τις Υψηλές τοποθεσίες για μια εφαρμογή Entersoft) και σύρσιμο μιας εφαρμογής από τη συσκευή. Για κάθε συσκευή που έχει εγγραφεί στο Entersoft core MDM Subsystem, υπάρχει ένα εκτεταμένο σύνολο εγγραφών Log και Audit Trail, καθώς και η τρέχουσα γνωστή κατάσταση της συσκευής σε σχέση με μια εφαρμογή Entersoft για κινητές συσκευές, όπως Τοποθεσία, UTC Datetime και άλλα σχετικά πεδία του περιβάλλοντος.

**Τα mobile apps μπορούν να φιλοξενηθούν σε private ή public app store;**

Οι Entersoft Mobile εφαρμογές δεν προσφέρονται μέσω των Public App Stores των Platform Vendors (π.χ. Google Play, Apple Store, Microsoft Store). Στην περίπτωση του Apple iOS, η εφαρμογή Entersoft Mobile for iOS υποστηρίζει πλήρως τα "Enterprise Stores" όπου ο Πελάτης είναι πλήρως υπεύθυνος για το Mobile Application (υπογραφή με τα πιστοποιητικά του, διαχείριση πιστοποιητικών διανομής και προφίλ κ.λπ.). Αυτό συνιστάται ιδιαίτερα για μεγάλες επιχειρήσεις και οργανισμούς.

**Το σύστημα ακολουθεί οποιαδήποτε ασφαλή πρακτική SDLC;**

Η Entersoft επιβάλλει πλήρως μια διαδικασία κύκλου ζωής ανάπτυξης λογισμικού τόσο στη διαδικασία ανάπτυξης προϊόντων όσο και στην υλοποίηση και προσαρμογή. Για κάθε sprint και S/W που πρόκειται να παραδοθεί, υπάρχουν φάσεις με πόρους, ρόλους και παραδοτέα που έχουν σχεδιαστεί για να προσφέρουν υψηλής ποιότητας λύσεις S/W και Υψηλές ποιότητας ποιότητας. Από την Ανάλυση Απαιτήσεων, τις Προδιαγραφές, τον Σχεδιασμό, την Υλοποίηση, τον Έλεγχο, Έλεγχο Ενσωμάτωσης, Έλεγχο Αποδοχής, έως τον Έλεγχο Ποιότητας υπάρχουν μεθοδολογίες, εργαλεία και αυτοματοποιημένα bots, κάτω από ένα καλά καθορισμένο σύνολο πολιτικών ασφαλείας σε μια ασφαλή και προστατευμένη ανάπτυξη περιβάλλοντος. Οι



	<p>διαδικασίες ανάπτυξης και παροχής υπηρεσιών Entersoft είναι πιστοποιημένες κατά ISO-9001/2015 &amp; ISO-20000/2018. Η ασφάλεια και η διαχείριση κινδύνων είναι βασικοί παράγοντες και για τα δύο πρότυπα και ελέγχονται κάθε χρόνο.</p>
<p>Το σύστημα υποβάλλεται σε τακτικούς ελέγχους ασφαλείας εφαρμογών;</p>	<p>Σε ετήσια βάση, τα προϊόντα λογισμικού της Entersoft SA και το Software as a service (SAAS) υποβάλλονται σε εκτεταμένες δοκιμές ευπάθειας (vulnerability tests), χρησιμοποιώντας ένα σύνολο εργαλείων και υπηρεσιών εκτίμησης ευπάθειας τεχνολογίας αιχμής (vulnerability assessment tools) που είναι εφαρμόσιμα για τις τεχνολογίες και τη φύση των υποσυστημάτων S/W κάθε προϊόντος.</p>