



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΦΕΤΕΙΟ ΑΘΗΝΩΝ**

ΣΥΜΒΑΣΗ

Για την ετήσια βελτιστοποίηση-εξελικτική συντήρηση και φιλοξενία της ιστοσελίδας του Εφετείου Αθηνών (www.efeteioathinon.gr)

Στην Αθήνα και στο Δικαστικό Μέγαρο του Εφετείου Αθηνών, σήμερα στις **5 Μαρτίου του έτους 2018**, ημέρα Δευτέρα και ώρα 13:30, οι παρακάτω συμβαλλόμενοι:

1. Ο Πρόεδρος του Τριμελούς Συμβουλίου που διευθύνει το Εφετείο Αθηνών, **Θεόδωρος Κανελλόπουλος Αρεοπαγίτης** και
2. Η ατομική επιχείρηση **«Γεώργιος Κων. Χρυσικός»** που εδρεύει στο Γαλάτσι Αττικής, οδός Ορφέως αρ. 5, Τ.Κ.111 46, τηλ. 210-2934060 Fax: 210-2934014, με Α.Φ.Μ.: 036318810, Δ.Ο.Υ. Γαλασίου και εκπροσωπείται από τον Γεώργιο Χρυσικό του Κωνσταντίνου που θα καλείται στο εξής **Ανάδοχος**,

συμφώνησαν και συναποδέχθηκαν τα ακόλουθα:

Το Εφετείο Αθηνών, προκειμένου να προβεί στην ετήσια **βελτιστοποίηση-εξελικτική συντήρηση και φιλοξενία της ιστοσελίδας του Εφετείου Αθηνών** (www.efeteioathinon.gr), βάσει των διατάξεων:

- α) Του άρθρου 64 του Ν.3900/2010 (ΦΕΚ Α' 213), «Εξορθολογισμός διαδικασιών και επιτάχυνση της διοικητικής δίκης και άλλες διατάξεις» όπως τροποποιήθηκε με την παρ. 2 του άρθρου 9 του Ν. 4022/2011 (ΦΕΚ 219 Α')
- β) Του Π.Δ. 80/2016 (ΦΕΚ Α' 145) και των άρθρων 66,68 και 91§2 του Ν.4270/2014 (Α' 143), «Αρχές δημοσιονομικής διαχείρισης και εποπτείας-δημόσιο λογιστικό και άλλες διατάξεις», όπως ισχύουν,

γ) του άρθρου 13 του ν.δ. 496/1974 «Περί Λογισμικού των Νομικών Προσώπων Δημοσίου Δικαίου» (ΦΕΚ Α' 204),

δ) Του Ν. 4412/2016 (Α' 147) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (Προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ»,

ε) την υπ' αριθμ. πρωτ. 100260/17-11-2011 κοινή Υπουργική Απόφαση των Υπουργών Οικονομικών και Δικαιοσύνης Διαφάνειας και Ανθρωπίνων Δικαιωμάτων.

2. Την υπ' αριθμ. Πρωτ. 5526/12-04-2017 απόφαση ανάληψης υποχρέωσης του ΤΑ.Χ.ΔΙ.Κ με την οποία εγκρίθηκε η επιχορήγηση του Εφετείου Αθηνών για την κάλυψη των λειτουργικών αναγκών αυτού και των υπηρεσιών αρμοδιότητάς του για το έτος 2017 (**ΑΔΑ:Ω9Γ846ΨΧΥΙ-1ΘΕ**),

3. Το υπ' αριθμ. Πρωτ. 6484/27-04-2017 Πρακτικό Καταμερισμού Τόκων 2016 της Επιτροπής Διαχείρισης Επιχορήγησης του Εφετείου Αθηνών (**ΑΔΑ:6Σ7Δ45Τ-ΘΡ3**)

4. Το με αριθμ. 147/10-11-2017 Πρακτικό συνεδρίασης της Τριμελούς Επιτροπής Διαχείρισης Επιχορηγήσεων του Εφετείου Αθηνών και το με αρ. πρωτ. 14662/11-10-2017(**ΑΔΑΜ: 17REQ002083044**) αίτημα του Εφετείου Αθηνών.

5. Το γεγονός ότι το ποσό της δεσμευόμενης, με την παρούσα, πίστωσης είναι εντός του εγκεκριμένου ποσού διάθεσης του προϋπολογισμού του Οικονομικού έτους 2017.

6. Την με αριθμό πρωτ. 16682/10-11-2017 (**ΑΔΑ:62Κ445Τ-ΨΧΜ, ΑΔΑΜ: 17REQ002310179**) απόφαση ανάληψης υποχρέωσης της Επιτροπής Διαχείρισης Επιχορήγησης του Εφετείου Αθηνών με την οποία εγκρίθηκε η δέσμευση πίστωσης ποσού ύψους τεσσάρων χιλιάδων τετρακοσίων σαραντατεσσάρων ευρώ και εξήντα έξι λεπτών (4.444,66 €) συμπεριλαμβανομένου του Φ.Π.Α σε βάρος του ΚΑΕ 02.01.0899.001 του προϋπολογισμού έτους 2017 (η οποία καταχωρήθηκε με α/α 77 στο Βιβλίο Εγκρίσεων και Εντολών Πληρωμής της Επιτροπής Διαχείρισης Επιχορήγησης του Εφετείου Αθηνών για την ετήσια βελτιστοποίηση- εξελικτική συντήρηση της ιστοσελίδας του Εφετείου Αθηνών (www.efeteioathinon.gr)).

7. Η ανωτέρω συντήρηση θα γίνει με τη διαδικασία της απευθείας ανάθεσης σύμφωνα με τις διατάξεις του άρθρου 64 του Ν.3900/2010, του Ν.4270/2014 και του Ν.4412/2016 και ειδικότερα των άρθρων 132 και 337 του Ν 4412/2016.

8. Την ανακοίνωση-πρόσκληση του Πρόεδρου του Τριμελούς Συμβουλίου Διεύθυνσης του Εφετείου Αθηνών, με αριθμό πρωτοκόλλου 2482/13-2-2018 για την

υποβολή των κατά νόμο απαραίτητων δικαιολογητικών από την ατομική επιχείρηση «Γεώργιος Κων. Χρυσικός»

9. Την από 8-02-2018 οικονομική προσφορά που κατατέθηκε στην υπηρεσία μας από την ατομική επιχείρηση «Γεώργιος Κων. Χρυσικός» για την ετήσια βελτιστοποίηση- εξελικτική συντήρηση της ιστοσελίδας του Εφετείου Αθηνών (www.efeteioathinon.gr).

10. Το γεγονός ότι η ιστοσελίδα του Εφετείου Αθηνών η οποία λειτουργεί από το έτος 2011, κατασκευάστηκε με έξοδα του Ταμείου Αλληλοβοήθειας των Δικαστών του Εφετείου Αθηνών, από τον Γ. Χρυσικό ως εξωτερικό συνεργάτη, λίγους μήνες πριν ολοκληρώθηκε η διαδικασία μεταβίβασης του domain name στο Εφετείο Αθηνών και υπάρχει πλέον αδήριτη ανάγκη αναβάθμισης της ιστοσελίδας αυτής προς κάλυψη των υπηρεσιακών αναγκών. Τούτο αποτελεί συμπληρωματικό έργο που κατέστη μεταγενεστέρως αναγκαίο και ως εκ τούτου δεν περιλαμβανόταν στην αρχική σύμβαση. Εν όψει των ανωτέρω, κατ' εφαρμογή των διατάξεων του άρθρου 132 παρ. 1β περ. αα, ββ και 337 παρ. 1β, βα, ββ του ν. 4412/2016, πρέπει να τροποποιηθεί η αρχική σύμβαση διατηρουμένου του αρχικού αναδόχου, εφόσον η αλλαγή αναδόχου δεν μπορεί να γίνει για οικονομικούς και τεχνικούς λόγους, αλλά και διότι θα συνεπαγόταν ως εκ της φύσεως του έργου σημαντικά προβλήματα, καθώς και ουσιαστική επικάλυψη δαπανών για την Αναθέτουσα Αρχή.

Στο πλαίσιο αυτό και στην προσπάθεια κάλυψης της ανάγκης για την βελτιστοποίηση-εξελικτική συντήρηση της ιστοσελίδας του Εφετείου Αθηνών, ζητήθηκε από τον εξωτερικό συνεργάτη που δημιούργησε και μέχρι σήμερα συντηρούσε την συγκεκριμένη ιστοσελίδα, προσφορά για τις ανωτέρω συνοπτικά περιγραφόμενες υπηρεσίες εξελικτικής συντήρησης αυτής, οι οποίες αποτελούν απαραίτητες προσαρμογές και βελτιώσεις τόσο σε θέματα ασφαλείας όσο και σε θέματα λειτουργικότητας που σε περίπτωση νέας υλοποίησης εξ αρχής θα συνεπαγόταν σημαντικά μεγαλύτερο κόστος για την υπηρεσία μας.

Το Τριμελές Συμβούλιο Διεύθυνσης του Εφετείου Αθηνών με την υπ' αριθμό **15/23-2-2018 Απόφασή του**, που αποτελεί αναπόσπαστο στοιχείο της παρούσης, ανέθεσε την σχετική συντήρηση στην ατομική επιχείρηση **«Γεώργιος Κων. Χρυσικός»** που εδρεύει στο Γαλάτσι Αττικής, οδός Ορφέως αρ. 5, Τ.Κ.111 46, τηλ. 210-2934060, Fax: 210-2934014, με Α.Φ.Μ.: 036318810, Δ.Ο.Υ. Γαλασίου, αντί

του συνολικού ποσού των τεσσάρων χιλιάδων τριακοσίων πενήντα εννιά ευρώ και δέκα λεπτών **#4.359,10#** € συμπεριλαμβανομένου του Φ.Π.Α. 24%.

Η Ανάδοχος εταιρία αναλαμβάνει την υλοποίηση της παρούσας σύμβασης η οποία, συντάχθηκε σύμφωνα με τις διατάξεις του Ν.4412/2016, τους όρους και τις τεχνικές προδιαγραφές που ορίζονται σε αυτήν, την οικονομική προσφορά της Αναδόχου εταιρίας και διέπεται από το ελληνικό δίκαιο, σύμφωνα με τους παρακάτω όρους:

Άρθρο 1^ο

ΑΝΤΙΚΕΙΜΕΝΟ ΣΥΜΒΑΣΗΣ – ΥΠΟΧΡΕΩΣΕΙΣ ΑΝΑΔΟΧΟΥ

Αντικείμενο της παρούσας αποτελεί η ετήσια **βελτιστοποίηση-εξελικτική συντήρηση και φιλοξενία της ιστοσελίδας του Εφετείου Αθηνών (www.efeteioathinon.gr)**, ως ακολούθως:

Η υλοποίηση του παρόντος έργου έχει ως στόχο την αναβάθμιση των ψηφιακών υπηρεσιών που προσφέρονται μέσα από την ιστοσελίδα του Εφετείου Αθηνών. Η υπάρχουσα ιστοσελίδα είναι κατασκευασμένη σε παλιότερη τεχνολογία **html frames** και δεν προσφέρει την απαραίτητη ασφάλεια, λειτουργικότητα και πληροφόρηση που θα έπρεπε να παρέχει. Οι κύριοι στόχοι και συνοπτικά οι προτάσεις για την επίτευξή τους είναι οι παρακάτω:

Αναβάθμιση Ασφαλείας.

- Η Μεταφορά της φιλοξενίας σε πιο ασφαλές περιβάλλον ενός Virtual Private Server
- Η Μεταφορά του υλικού που υπάρχει από html σε CMS WORDPRESS
- Η Εγκατάσταση πρωτοκόλλου κρυπτογράφησης μετάδοσης δεδομένων SSL
- Η Εγκατάσταση πρόσθετου ασφαλείας στο CMS WORDPRESS
- Η αυστηρή εφαρμογή των «Γενικών οδηγιών προστασίας διαδικτυακής υποδομής» της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων.

- Η πρόσβαση των χρηστών με συγκεκριμένους ρόλους και δικαιώματα.
- Η διαχείριση των κωδικών ασφαλείας των διαχειριστών, σύμφωνα με πολύ αυστηρά πρότυπα.
- Η Τακτική ενημέρωση όλων των ψηφιακών δομών (server, cms, plugins) και η καθημερινή λήψη αντιγράφων ασφαλείας.

Αναβάθμιση Παρεχόμενων πληροφοριών και υπηρεσιών

- Η δομή των ιστοσελίδων και η πρόσβαση σε αυτές να είναι ιδιαίτερα εύχρηστη και λειτουργική.
- Η παρουσία των πληροφοριών της ιστοσελίδας να είναι πλήρως συμβατή “full responsibility” με όλες τις συσκευές που έχουν πρόσβαση στο internet (Ηλεκτρονικοί υπολογιστές, Tablets, κινητά τηλέφωνα)
- Η ιστοσελίδα να είναι πλήρως συμβατή με το πρότυπο WCAG 2.0 για προσβασιμότητα ΑΜΕΑ.
- Στην ιστοσελίδα να προστεθούν νέες ενότητες πληροφόρησης του κοινού ανά διοικητικό τμήμα του Εφετείου Αθηνών ή άλλης κατηγοριοποίησης.
- Να προστεθούν νέες ψηφιακές υπηρεσίες προς τους συνηγόρους και τους πολίτες που μέσα από διαβαθμισμένη πρόσβαση να έχουν την δυνατότητα κατάθεσης εντύπων και αιτήσεων προς τα τμήματα του Εφετείου Αθηνών.
- Να προστεθεί το απαραίτητο plugin που θα επιτρέπει τη δημιουργία πλατφόρμας ασύγχρονης εκπαίδευσης MOODLE
- Να γίνει εκπαίδευση του προσωπικού του Εφετείου Αθηνών στην χρήση της ιστοσελίδας και των δεδομένων που θα λαμβάνουν

- Να γίνει συμμόρφωση με τον νέο ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (gdpr) όπου απαιτείται.

1. Αρχιτεκτονική της Προσφερόμενης Λύσης

Γενικές Αρχές Αρχιτεκτονικής Λογισμικού

Ο αρχιτεκτονικός σχεδιασμός και η ανάπτυξη της Πύλης θα ενσωματώνει και θα υλοποιεί τα ακόλουθα βασικά χαρακτηριστικά που προσφέρει το ανοιχτό σύστημα διαχείρισης περιεχομένου CMS Wordpress.

1. Αρθρωτή (modular) αρχιτεκτονική που βασίζεται σε εικαστικό θέμα και πρόσθετα, ώστε να επιτρέπονται μελλοντικές επεκτάσεις και αντικαταστάσεις, ενσωματώσεις, αναβαθμίσεις ή αλλαγές διακριτών τμημάτων λογισμικού.
2. Αρχιτεκτονική 3-tier (web-application-database) για την ευελιξία της κατανομής φορτίου, την αποδοτική εκμετάλλευση των χαρακτηριστικών ασφαλείας του περιβάλλοντος «φιλοξενίας» (hosting) και την ευκολία στην επεκτασιμότητα.
3. Διαβαθμισμένη πρόσβαση ανάλογα με το είδος των υπηρεσιών και την ταυτότητα των χρηστών.

Τα επίπεδα πρόσβασης είναι τα παρακάτω:

- Επίπεδο διαχειριστή domain name.

Ο λογαριασμός αυτός έχει πρόσβαση στον ορισμό των DNS εγγραφών του Server.

- Επίπεδο Επιχειρησιακού Διαχειριστή Server (Server Operational Administrator): Ο λογαριασμός αυτός έχει την πλήρη πρόσβαση στις λειτουργίες και δυνατότητες του Server.
- Επίπεδο Τεχνικού Διαχειριστή Server (Technical Administrator): Ο λογαριασμός αυτός δίνει δικαιώματα στο διαχειριστή του server να εκτελεί τακτικές εργασίες συντήρησης και αναβάθμισης. Μπορεί να εισάγει νέους χρήστες, να διαγράψει υπάρχοντες και να προχωράει γενικά σε αλλαγές της παραμετροποίησης του συστήματος όπως είναι προσθήκη νέων διευθύνσεων, αλλαγή οργανωτικής δομής κτλ.
- Επίπεδο Τοπικών Χρηστών (Local Users): Ο λογαριασμός αυτός είναι για τους απλούς εσωτερικούς χρήστες της ΥΠΗΡΕΣΙΑΣ και μπορεί να έχει δύο επίπεδα διαβάθμισης. Το πρώτο επίπεδο θα μπορούσε να είναι του απλού χρήστη και το δεύτερο του έχοντος την ευθύνη κάποιας συγκεκριμένης υπηρεσίας.
- Επίπεδο Εξωτερικών Χρηστών (External Users): Ο λογαριασμός αυτός είναι για τους χρήστες του εξωστρεφούς μέρους της ιστοσελίδας που είναι οι Δικηγόροι και οι πολίτες. Ο λογαριασμός αυτός μπορεί να έχει επίσης περισσότερα επίπεδα. Τα επίπεδα αυτά μπορεί να διαμορφώνονται ανάλογα με τις υπηρεσίες οι οποίες μπορούν να κατηγοριοποιηθούν με το βαθμό κρισιμότητας της πραγματικής ταυτότητας του εξωτερικού χρήστη. Είναι ευνόητο ότι δεν έχουν όλες οι υπηρεσίες την ίδια κρισιμότητα ως προς το συγκεκριμένο κριτήριο.

Όπου απαιτείται θα εξασφαλίζεται η ασφάλεια της μεταφοράς δεδομένων από και προς την ιστοσελίδα μέσω SSL πρωτοκόλλου.

2. Αναβάθμιση ανασχεδιασμός της ιστοσελίδας.

- Η ιστοσελίδα θα αναπτυχθεί σε cms wordpress στην τελευταία σταθερή Ελληνική έκδοση 4.8.2 <https://el.wordpress.org/>
- Η εικαστική και λειτουργική δόμηση θα υποστηριχθεί με το θέμα DIVI 3 της ELEGANT THEMES <https://www.elegantthemes.com/gallery/>
- Για την ασφάλιση της ιστοσελίδας θα εγκατασταθεί και θα παραμετροποιηθεί το πρόσθετο firewall Sucuri PRO <https://sucuri.net/>
- Για την επικοινωνία με τους δικηγόρους και το κοινό θα χρησιμοποιηθεί το πρόσθετο **Gravity Forms Pro** <http://www.gravityforms.com/>

Ο ανασχεδιασμός της Ιστοσελίδας θα εξασφαλίζει:

- Την ενίσχυση της εικόνας της ΥΠΗΡΕΣΙΑΣ με μία καλαίσθητη εικαστική παρουσίαση.
- Την ευκολία ανανέωσης και την γρήγορη και δυναμική παρουσίαση των πληροφοριών.
- Την εύκολη και γρήγορη πρόσβαση στην πληροφορία.

Η Ιστοσελίδα θα διαθέτει τα ακόλουθα χαρακτηριστικά:

- Ένα κατανοητό σύστημα πλοήγησης και θεματολογίας. Ο χρήστης θα μπορεί να κινείται άνετα ανάμεσα σε περιλήψεις του περιεχομένου και σε λεπτομερή και δομημένη ανάπτυξη αυτού.
- Δυνατότητα πρόσβασης σε ιεραρχικούς καταλόγους εγγράφων και αρχείων περιεχομένου σύμφωνα με πολλαπλή θεματική κατηγοριοποίηση,

με μορφή καταλόγων και πολλαπλών μορφών ενός εκάστου εγγράφου (DOC, PDF, XLS).

- Ευέλικτη αναζήτηση στο περιεχόμενο (από πολλαπλές, δομημένες και αδόμητες πηγές) της πύλης βάσει πολυκριτηριακών πληροφοριών (λέξεις κλειδιά, θέμα, κείμενο, ημερομηνία κλπ.).
- Αναγνώριση και αυθεντικοποίηση των δικηγόρων – χρηστών.
- Πρόσβαση σε συγκεκριμένα μόνο στοιχεία την βάσης δεδομένων τα οποία θα αφορούν τον εξουσιοδοτημένο χρήστη.
- Χάρτη του δικτυακού τόπου (site map), θα παρουσιάζει τη δομή της πύλης, ώστε να μπορεί ο επισκέπτης να δει τι περιέχει κάθε ενότητα, και να πλοηγείται γρήγορα και εύκολα.
- Πρόσβαση από ΑΜΕΑ Στη σχεδίαση και υλοποίηση θα ληφθούν υπόψη οι ιδιαίτερες ανάγκες και απαιτήσεις πρόσβασης στις αναπτυσσόμενες εφαρμογές και υπηρεσίες από ΑΜΕΑ και άλλες ευπαθείς ομάδες πληθυσμού, και θα εφαρμοστούν, όπου υπάρχουν, οι σχετικοί διεθνώς αναγνωρισμένοι κανόνες και οδηγίες προσβασιμότητας (όπως ενδεικτικά του Web Accessibility Initiative και συγκεκριμένα Web Content Accessibility Guidelines 1.0 Authoring Tool Accessibility Guidelines 1.0 User Agent Accessibility Guidelines 1.0 – <http://www.w3.org/TR/WCAG10/> <http://www.w3.org/TR/WCAG10>) που αφορούν την ανάπτυξη προσβάσιμων εφαρμογών και υπηρεσιών σε περιβάλλον Παγκόσμιου Ιστού. Επιπλέον θα πρέπει να ληφθούν υπόψη όλες οι διεθνείς προδιαγραφές και τεχνικές που περιγράφονται από το World Wide Web Consortium (W3C) στην οδηγία Web Accessibility Initiative (WAI) που αφορά την πρόσβαση ΑΜΕΑ σε ιστοσελίδες. Η νέα ιστοσελίδα της ΥΠΗΡΕΣΙΑΣ είναι υποχρεωτικό να έχει πιστοποίηση επιπέδου τουλάχιστον AA (double A), όπως αυτή καθορίζεται από το W3C.

- Στην ιστοσελίδα θα υπάρχουν 4 τομείς ενημέρωσης που επιγραμματικά αναλύονται παρακάτω, ενώ ένα λειτουργικό περιβάλλον δοκιμών θα είναι προσβάσιμο στο url: <http://efeteio.madlink.gr/>
- ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ Στην περιοχή αυτή θα υπάρχουν όλες οι στατικές πληροφορίες που υπάρχουν και τώρα στην ιστοσελίδα όπως ιστορικό, διοίκηση, πρόσβαση, επικοινωνία κλπ.
- ΕΝΗΜΕΡΩΣΗ Στην περιοχή αυτή θα υπάρχει όλη η τρέχουσα πληροφόρηση που σε δημοσιεύει το Εφετείο Αθηνών (π.χ. Ανακοινώσεις, ποινικές έδρες κλπ)
- Δύο περιοχές όπου θα υπάρχει η δυνατότητα οι επισκέπτες της ιστοσελίδας να έχουν ηλεκτρονικές υπηρεσίες εξυπηρέτησης μέσα από ψηφιακή κατάθεση αιτήσεων ή άλλων σχετικών έγγραφων για διάφορες διαδικασίες που υπάρχουν στο Εφετείο Αθηνών. Οι υπηρεσίες αυτές μπορούν να προσφέρονται είτε σε πιστοποιημένους χρήστες (π.χ. συνήγοροι) ή ελεύθερα στο κοινό. Σε κάθε περίπτωση θα τηρούνται όλες οι απαιτήσεις ασφαλείας.

Σελίδα δοκιμών σε πραγματικό περιβάλλον.

Η προτεινόμενη νέα δομή της ιστοσελίδας καθώς και η εξελικτική διαδικασία διαμόρφωσής της θα γίνεται στο δοκιμαστικό περιβάλλον <http://efeteio.madlink.gr> Το ίδιο περιβάλλον θα χρησιμοποιηθεί για την εκπαίδευση των χρηστών, καθώς και για την δημιουργία σεναρίων δοκιμών.

Υπογραφή κατασκευαστή ιστοσελίδας.

Στο τελευταίο τμήμα της ιστοσελίδας και μετά το υποσέλιδο θα αναγράφεται με διακριτική γραφή ως υπογραφή κατασκευαστή το παρακάτω κείμενο «Κατασκευή και υποστήριξη ιστοσελίδας Madlink 2018»

με ενεργό υπερσύνδεσμο στην σελίδα του κατασκευαστή, όπως υπάρχει και στην παρούσα ιστοσελίδα.

3. Ανάλυση εργασιών εξελικτικής συντήρησης για την αναβάθμιση της φιλοξενίας και της δομής της ιστοσελίδας.

Εργασίες αναβάθμισης φιλοξενίας

- Διαμόρφωση λειτουργικού λογισμικού (Centos 7.3 Plesk 17.5) νέας φιλοξενίας για την υποδοχή της νέας ιστοσελίδας. Η διαμόρφωση του Centos Plesk θα γίνει σύμφωνα με τις Γενικές Οδηγίες Προστασίας Διαδικτυακής Υποδομής της εθνικής αρχής αντιμετώπισης ηλεκτρονικών επιθέσεων
- Διαμόρφωση και κατανομή πόρων συστήματος για την μέγιστη απόδοση του.
- Δημιουργία νέων λογαριασμών email σύμφωνα με την κατάσταση ενεργών email που θα μας δοθεί από το Εφετείο Αθηνών. Οι νέοι λογαριασμοί που θα δημιουργηθούν θα επικοινωνούν με τους χρήστες μέσω πρωτοκόλλου POP και θα έχουν μέγιστο όριο που θα μας οριστεί από το Εφετείο Αθηνών. Όλοι οι νέοι λογαριασμοί θα λάβουν νέους κωδικούς πρόσβασης που θα πρέπει να αλλαχθούν άμεσα από τους χρήστες τους με κωδικούς δικής τους επιλογής.
- Κατά την διάρκεια της μετάπτωσης των DNS εγγραφών (τελική κίνηση για την μεταφορά από την παλιά φιλοξενία στην νέα) θα πρέπει γίνει περιορισμένη χρήση των emails, ενώ θα πρέπει να έχει προηγηθεί κατέβασμα των emails στους κατά τόπους Η/Υ. Ο χρόνος μετάπτωσης κυμαίνεται από 3 έως 48 ώρες.

- Εκπαίδευση μηχανογράφων διαχειριστών για την διαχείριση των email λογαριασμών.
- Εγγραφή και μετάπτωση domain στην νέα φιλοξενία και ιστοσελίδα (αλλαγή dns) σε χρόνο που θα μας καθορίσει το Εφετείο Αθηνών και εκτός εργάσιμων ημερών για να υπάρξει η μικρότερη δυνατή αναστάτωση.

Εργασίες αναβάθμιση ιστοσελίδας

- Εγκατάσταση και παραμετροποίηση Wordpress, Εικαστικού Θέματος και Πρόσθετων. Η εγκατάσταση και παραμετροποίηση θα γίνει σύμφωνα με τις Γενικές Οδηγίες Προστασίας Διαδικτυακής Υποδομής της εθνικής αρχής αντιμετώπισης ηλεκτρονικών επιθέσεων.
- Διαμόρφωση εικαστικού θέματος (Divi 3) και διαμόρφωση του. Η εικαστική διαμόρφωση θα γίνει έτσι ώστε να τονίζει το κύρος του Εφετείου Αθηνών. Οι χρωματικοί συνδυασμοί που θα χρησιμοποιηθούν θα είναι σε τόνους του λευκού και του γαλάζιου. Η λειτουργική διαμόρφωση θα γίνει έτσι ώστε να είναι ιδιαίτερα εύκολη η πρόσβαση στην πληροφόρηση. Η εμφάνιση και η λειτουργικότητα της σελίδας θα είναι το ίδιο αποδοτική σε όλες τις συσκευές που έχουν πρόσβαση στο ιντερνέτ ανεξάρτητα από το μέγεθος ή την γεωμετρία της εμφάνισης (full responsibility). Η ιστοσελίδα να είναι πλήρως συμβατή με το πρότυπο WCAG 2.0 για προσβασιμότητα ΑΜΕΑ.
- Μεταφορά υλικού και αναδιαμόρφωση του σύμφωνα με τις απαιτήσεις του νέου θέματος και της νέας τεχνολογίας. Η μεταφορά των σελίδων θα γίνει με πλήρη νέα διαμόρφωση της σελίδας. Η μεταφορά της αρθρογραφίας και της συνεχούς ροής πληροφόρησης θα γίνει με μεταφορά του υπάρχοντος υλικού και αναδιαμόρφωση των δομών πρόσβασης στην πληροφόρηση που παραμένει στο πρωταρχικό υλικό.

- Εγκατάσταση και παραμετροποίηση κυκλώματος πρόσβασης διαβαθμισμένων χρηστών (συνήγοροι).
- Εγκατάσταση και παραμετροποίηση έως 3 φορμών επικοινωνίας – κατάθεσης αιτήσεων ή εγγράφων διαβαθμισμένων ή ελεύθερων χρηστών με τα αντίστοιχα τμήματα που θα μας υποδείξει το Εφετείο Αθηνών.
 - ο Οι φόρμες επικοινωνίας θα διαμορφωθούν σύμφωνα με τις απαιτήσεις και τις προδιαγραφές λειτουργίας του Εφετείου Αθηνών και του ανάλογου τμήματος.
 - ο Πρόσβαση στην πληροφόρηση από την φόρμα επικοινωνίας θα έχουν οι χρήστες του κάθε τμήματος μέσα από εισερχόμενα emails στο λογαριασμό τους στο @efeteioathinon.gr
 - ο Πρόσβαση στις εγγραφές των φορμών επικοινωνίας και εξαγωγή τους για περαιτέρω ανάλυση θα έχουν οι προϊστάμενοι των τμημάτων ή όποιος οριστεί.
 - ο Εκπαίδευση διαχειριστών στην χρήση των φορμών επικοινωνίας και των εγγράφων τους. Ενημερωτική πληροφόρηση των χρηστών σχετικά με τα πληροφοριακά email που θα λαμβάνουν.
 - ο Η εγκατάσταση και παραμετροποίηση νέων φορμών πέραν των πρώτων 3 θα χρεώνεται σύμφωνα με τον πίνακα κόστους μηχανογραφικών ανθρωποωρών της οικονομικής προσφοράς.
 - ο Για την δημιουργία των φορμών επικοινωνίας θα πρέπει να υπάρξει συνεργασία ενημέρωσης με τους προϊσταμένους των τμημάτων που θα έχουν την φόρμα.
- Τέλος θα γίνουν δοκιμές λειτουργίας των ιστοσελίδων των δομών και των φορμών επικοινωνίας που θα πιστοποιήσουν την λειτουργικότητα και την ασφάλεια τους.

4. Εκπαίδευση στη Χρήση του Συστήματος

Θα προκύψει εκπαίδευση των διαχειριστών και των διαβαθμισμένων χρηστών της ιστοσελίδας συνολικής διάρκειας είκοσι 20 ωρών.

Η εκπαίδευση θα γίνει βάση σχεδίου εκπαίδευσης και σε συνεργασία με την Αναθέτουσα Αρχή. Στο σχέδιο που θα υποβληθεί από την εταιρεία θα αναφέρονται αναλυτικά τα αντικείμενα της εκπαίδευσης, η διάρκεια και η περιγραφή των αντικειμένων.

Η εκπαίδευση των χρηστών περιλαμβάνει τα στελέχη Πληροφορικής του τμήματος Μηχανοργάνωσης της ΥΠΗΡΕΣΙΑΣ. Η εκπαίδευση αυτή θα υποστηριχθεί από υλικό σε έντυπη ή ηλεκτρονική μορφή, το οποίο θα παραμείνει στη διάθεσή τους για όλο το διάστημα χρήσης του συστήματος.

Η εταιρεία θα παράσχει εγχειρίδιο χρήστη (user's manual) με την μορφή on-line help και εγχειρίδιο διαχειριστή (administrator's manual) σε έντυπη και/ ή ηλεκτρονική μορφή.

Η εκπαίδευση θα περιλαμβάνει ενδεικτικά τις παρακάτω ενότητες:

Διαχείριση συστήματος : 4 ώρες

- Διαχείριση server (Εκπαίδευση μηχανογράφων διαχειριστών για την διαχείριση των email λογαριασμών.)
- Διαχείριση Wordpress πρόσθετων και αναβαθμίσεων

Υποσύστημα Περιεχομένου: 6 ώρες

- Διαχείριση Περιεχομένου, Ενότητες, Κατηγορίες, Στοιχεία Περιεχομένου.

- Διαχείριση Σελίδων, άρθρων, και όλων των ενοτήτων πληροφόρησης.
- Διαχείριση πρόσθετων και ρυθμίσεις αυτών.
- Διαχείριση Θέματος εικαστικών παρεμβάσεων.
- Διαχείριση Gravity forms.

Υποσύστημα φορμών επικοινωνίας: 10 ώρες

- Εκπαίδευση στην λειτουργία του email που θα λαμβάνει την πληροφόρηση.
- Εκπαίδευση προϊσταμένου Διαχείριση του τμήματος στην διαχείριση της βάση των αιτήσεων – επικοινωνιών.

5. Στατιστικά - Ανάλυση Χρήσης ιστοσελίδας.

Η ιστοσελίδα θα παρέχει παρέχει στατιστικά χρήσης μέσα από την υπηρεσία Google Analytics ώστε να είναι δυνατή η βελτίωση της συνολικής αποτελεσματικότητάς της και η εξαγωγή χρήσιμων συμπερασμάτων. Θα είναι δυνατή η εξαγωγή μηνιαίων, τριμηνιαίων, εξαμηνιαίων και ετήσιων στατιστικών λειτουργίας της Πύλης όπως:

- Αριθμός επισκέψεων
- Αριθμός μοναδικών επισκεπτών
- Αριθμός επισκέψεων ανά σελίδα
- Αριθμός συνολικών hits
- Αριθμός μεγέθους (bytes) πληροφορίας που εξάγεται από την Πύλη
- Κατανομή αριθμού επισκέψεων ανά ώρα, ημέρα, εβδομάδα, κτλ. με γραφικές απεικονίσεις.

Τα στατιστικά στοιχεία επισκεψιμότητας, θα είναι προσβάσιμα από επιλεγμένους διαχειριστές.

6. Λειτουργία και Συντήρηση

Η Λειτουργία και συντήρηση προσφέρεται σε ετήσια βάση με ημερομηνία έναρξης την ημερομηνία υπογραφής της σύμβασης και λήξη ένα έτος μετά. Το κόστος λειτουργίας και συντήρησης περιλαμβάνεται στο ετήσιο κόστος λειτουργίας της ιστοσελίδας.

Υποστήριξη Server

Κατά τις εργάσιμες ώρες και ημέρες

- Εγκατάσταση ενημερώσεων λογισμικών και λειτουργικού λογισμικού
- Επίβλεψη χρήσης πόρων και ρύθμιση της κατανομής τους
- Τηλεφωνική και On-line υποστήριξη διαχειριστών Εφετείου Αθηνών σε θέματα που αφορούν την διαχείριση του server

Πέραν των εργάσιμων ωρών

- Δημιουργία αντιγράφων ασφαλείας του συστήματος καθημερινά στον server και διατήρηση mirror αντιγράφων σε απομακρυσμένο server με συνολικό χώρο έως 160 Gbyte
- Άμεση επίλυση θεμάτων που αφορούν την ασφάλεια και την εξασφάλιση διαρκούς επιχειρησιακής λειτουργίας της ιστοσελίδας.

Υποστήριξη ιστοσελίδας

- Εγκατάσταση ενημερώσεων Wordpress θεμάτων προσθέτων
- Επίβλεψη χρηστών διαχείρισης ιστοσελίδας και υλικού που ανεβαίνει.
- Τηλεφωνική και On-line υποστήριξη διαχειριστών φορμών επικοινωνίας

- Τηλεφωνική και On-line υποστήριξη διαχειριστών Εφετείου Αθηνών σε θέματα που αφορούν την διαχείριση της ιστοσελίδας.

7. Χρονοδιάγραμμα Έργου

Η διάρκεια υλοποίησης του έργου της εξελικτικής συντήρησης αναβάθμισης της ιστοσελίδας του Εφετείου Αθηνών θα είναι τρεις (3) μήνες, από την υπογραφή της σύμβασης με την ΥΠΗΡΕΣΙΑ. Οι υπηρεσίες φιλοξενίας και τεχνικής υποστήριξης είναι ετήσιας διάρκειας.

Το συνολικό ενδεικτικό χρονοδιάγραμμα έχει ως εξής:

ΦΑΣΕΙΣ / ΕΡΓΑΣΙΕΣ ΔΙΑΡΚΕΙΑ

Φάση 1η	Διαμόρφωση Server, εγκατάσταση wordpress, πρόσθετων	Εντός 2 εβδομάδων μετά την υπογραφή σύμβασης
Φάση 1η	Δημιουργία λογαριασμών email στο νέο server	Εντός 3 εβδομάδων μετά την υπογραφή σύμβασης
Φάση 1η	Διαμόρφωση πρότασης εικαστικής απεικόνισης, έλεγχος από την υπηρεσία και οριστικοποίηση εμφάνισης.	Εντός 2 εβδομάδων μετά την υπογραφή σύμβασης
Φάση 2η	Μεταφορά υλικού από παλιά δομή ιστοσελίδας στη νέα που θα έχει επιλεγεί.	Εντός 2 μηνών μετά την υπογραφή σύμβασης
Φάση 2η	Ανάλυση απαιτήσεων και δημιουργία έως 3 φορμών επικοινωνίας. Έναρξη εκπαίδευση χρηστών και διαχειριστών	Εντός 2 μηνών μετά την υπογραφή σύμβασης

Φάση 3η	Πιλοτική λειτουργία για χρονικό διάστημα 2 εβδομάδων, έλεγχος λειτουργικότητας φορμών. Γενικός έλεγχος απαιτήσεων ασφαλείας. Ολοκλήρωση εκπαίδευσης.	Εντός 3 μηνών μετά την υπογραφή σύμβασης
Φάση 3η	Αλλαγή DNS εγγραφών στο efeteioathinon.gr	3 μήνες μετά την υπογραφή της σύμβασης και σε χρόνο που θα συναποφασιστεί

Η διάρκεια υλοποίησης του έργου της εξελικτικής συντήρησης αναβάθμισης της ιστοσελίδας του Εφετείου Αθηνών θα είναι τρεις (3) μήνες, από την υπογραφή της σύμβασης με την ΥΠΗΡΕΣΙΑ. Οι υπηρεσίες φιλοξενίας και τεχνικής υποστήριξης-συντήρησης της αναβαθμισμένης ιστοσελίδας είναι ετήσιας διάρκειας.

Το συνολικό ενδεικτικό χρονοδιάγραμμα έχει ως εξής:

ΦΑΣΕΙΣ / ΕΡΓΑΣΙΕΣ ΔΙΑΡΚΕΙΑ

Φάση 1η	Διαμόρφωση Server, εγκατάσταση wordpress, πρόσθετων	Εντός 2 εβδομάδων μετά την υπογραφή σύμβασης
Φάση 1η	Δημιουργία λογαριασμών email στο νέο server	Εντός 2 εβδομάδων μετά την υπογραφή σύμβασης
Φάση 1η	Διαμόρφωση πρότασης εικαστικής απεικόνισης, έλεγχος από την υπηρεσία και οριστικοποίηση εμφάνισης.	Εντός 2 εβδομάδων μετά την υπογραφή σύμβασης
Φάση 2η	Μεταφορά υλικού από παλιά δομή ιστοσελίδας στη νέα που θα έχει επιλεγεί.	Εντός 1 μηνός μετά την υπογραφή

		σύμβασης
Φάση 2η	Ανάλυση απαιτήσεων και δημιουργία έως 3 φορμών επικοινωνίας. Έναρξη εκπαίδευση χρηστών και διαχειριστών	Εντός 2 μηνών μετά την υπογραφή σύμβασης
Φάση 3η	Πιλοτική λειτουργία για χρονικό διάστημα 4 εβδομάδων, έλεγχος λειτουργικότητας φορμών. Γενικός έλεγχος απαιτήσεων ασφαλείας. Ολοκλήρωση εκπαίδευσης.	Εντός 3 μηνών μετά την υπογραφή σύμβασης
Φάση 3η	Αλλαγή DNS εγγραφών στο efeteioathinon.gr	Μετά από 3 μήνες μετά την υπογραφή σύμβασης και σε χρόνο που θα συναποφασιστεί

ΑΡΘΡΟ 2^ο

ΠΟΣΟ ΣΥΜΒΑΣΗΣ - ΤΡΟΠΟΣ ΠΛΗΡΩΜΗΣ-ΚΡΑΤΗΣΕΙΣ

(άρθρο 200 του Ν.4412/2016)

Ως συνολική τιμή συμφωνείται το ποσό των τεσσάρων χιλιάδων τριακοσίων πενήντα εννιά ευρώ και δέκα λεπτών **#4.359,10#** € συμπεριλαμβανομένου του Φ.Π.Α. 24%

Οι πιστώσεις βαρύνουν την πίστωση του προϋπολογισμού εξόδων του ειδικού λογαριασμού που διαχειρίζεται η Επιτροπή Διαχείρισης του Εφετείου Αθηνών, και συγκεκριμένα τον **ΚΑΕ 02.01.0899.001**, οικονομικού έτους 2017.

Ι. Τρόπος πληρωμής

Η καταβολή στην Ανάδοχο εταιρία του τιμήματος των παρεχόμενων υπηρεσιών θα γίνεται τμηματικά για το 100% της αξίας του εκάστοτε Δελτίου Παροχής Υπηρεσιών, που θα εκδίδεται **ανά τρίμηνο** μετά την οριστική παραλαβή της προσφερόμενης υπηρεσίας από την αρμόδια Επιτροπή Παραλαβής που έχει συσταθεί με απόφαση του Προϊσταμένου του Εφετείου Αθηνών, κατ' άρθρο 221 του Ν.4412/2016, η οποία (Επιτροπή) θα συντάσσει τη βεβαίωση καλής εκτέλεσης

εργασιών και θα την αποστέλλει στη συνέχεια στο Εφετείο Αθηνών – Επιτροπή Διαχείρισης της Επιχορήγησης.

Ειδικότερα ορίζεται ότι η πρώτη πληρωμή (Α τρίμηνο) θα αφορά στο 50% του συνολικού τιμήματος συμπεριλαμβανομένου ΦΠΑ και το υπόλοιπο ποσό θα πληρωθεί σε τρεις ισόποσες πληρωμές.

Η καταβολή του ποσού θα γίνεται από τη Τριμελή Επιτροπή Διαχείρισης της Επιχορήγησης του Εφετείου Αθηνών με τραπεζική επιταγή της Alpha Bank, μετά την υποβολή των απαιτούμενων δικαιολογητικών όπως αναφέρονται στο άρθρο 200 του Ν. 4412/2016.

II. Δικαιολογητικά πληρωμής σε συμβάσεις υπηρεσιών

Για την πληρωμή του τιμήματος απαιτούνται κατ' ελάχιστον τα εξής δικαιολογητικά:

- α) Πρωτόκολλο οριστικής παραλαβής του τμήματος που αφορά η πληρωμή,
- β) Τιμολόγιο του αναδόχου, που θα εκδίδεται στο όνομα του Εφετείου Αθηνών, Διεύθυνση: Κυρίλλου Λουκάρεως, αρ.14, Τ.Κ. 11522 Αθήνα , και Α.Φ.Μ. 997414035 - Δ.Ο.Υ. Ψυχικού
- γ) Εξοφλητική απόδειξη του αναδόχου, εάν το τιμολόγιο δεν φέρει την ένδειξη «Εξοφλήθηκε»,
- δ) Πιστοποιητικά Φορολογικής και Ασφαλιστικής Ενημερότητας.

Πέραν των ανωτέρω δικαιολογητικών οι αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή, μπορούν να ζητήσουν και οποιοδήποτε άλλο δικαιολογητικό. (άρθρο 200 παρ.6 του Ν.4412/16).

III. Κρατήσεις

Από το ποσό της συνολικής αμοιβής θα γίνει παρακράτηση φόρου υπηρεσιών 8% καθώς και των νόμιμων κρατήσεων, οι οποίες βαρύνουν τον ανάδοχο, σύμφωνα με τις ισχύουσες κάθε φορά σχετικές διατάξεις, και συγκεκριμένα την κράτηση 0,06% υπέρ της Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων (Ε.Α.Α.ΔΗ.ΣΥ.), η οποία υπολογίζεται επί της συνολικής συμβατικής καθαρής αξίας των ειδών, προ φόρων και κρατήσεων (άρθ. 375 παρ. 7 ν. 4412/16), καθώς και την κράτηση (0,06%) υπέρ Α.Ε.Π.Π. (άρθ. 350 παρ. 3 ν. 4412/16). Η κράτηση υπέρ Ε.Α.Α.ΔΗ.ΣΥ. υπάγεται σε χαρτόσημο 3% και Ο.Γ.Α. χαρτοσήμου, που υπολογίζεται με ποσοστό 20% επί του χαρτοσήμου.

ΑΡΘΡΟ 3^ο

ΧΡΟΝΟΣ ΕΝΑΡΞΗΣ – ΔΙΑΡΚΕΙΑ - ΟΛΟΚΛΗΡΩΣΗ ΕΚΤΕΛΕΣΗΣ ΣΥΜΒΑΣΗΣ

(άρθρα 38, 217, 202 του Ν.4412/2016)

Χρόνος έναρξης εκτέλεσης του παρόντος συμφωνητικού ορίζεται η ημερομηνία ανάρτησής του στο ΚΗΜΔΗΣ (άρθρο 38, παρ.7 του Ν.4412/2016).

Η χρονική διάρκεια του παρόντος συμφωνητικού ορίζεται από **5-03-2018 έως 4-03-2019.**

Ολοκλήρωση εκτέλεσης σύμβασης

Η σύμβαση θεωρείται ότι εκτελέστηκε όταν συντρέχουν οι εξής προϋποθέσεις:

- α. Οι υπηρεσίες συντήρησης παρασχέθηκαν στο σύνολό τους ,
- β. Παραλήφθηκαν οριστικά ποσοτικά και ποιοτικά οι υπηρεσίες που παραδόθηκαν.
- γ. Έγινε η αποπληρωμή του συμβατικού τιμήματος, αφού προηγουμένως επιβλήθηκαν κυρώσεις ή εκπτώσεις και
- δ. Εκπληρώθηκαν και οι λοιπές συμβατικές υποχρεώσεις και από τα δύο συμβαλλόμενα μέρη κατά τα προβλεπόμενα από τη σύμβαση. (άρθρο 202 του Ν.4412/2016)

ΑΡΘΡΟ 4°

ΠΑΡΑΛΑΒΗ ΥΠΗΡΕΣΙΩΝ – ΑΠΟΡΡΙΨΗ ΠΑΡΑΔΟΤΕΟΥ – ΑΝΤΙΚΑΤΑΣΤΑΣΗ

(άρθρα 219, 220 του Ν.4412/2016)

Η παραλαβή των υπηρεσιών συντήρησης θα γίνει από την Επιτροπή Παραλαβής της παρ. 5 του άρθρου 221 του ν. 4412/2016, η οποία συγκροτείται στο Εφετείο Αθηνών.

Αν η Επιτροπή Παραλαβής κρίνει ότι οι παρεχόμενες υπηρεσίες δεν ανταποκρίνονται πλήρως στους όρους της παρούσας σύμβασης, συντάσσεται πρωτόκολλο προσωρινής παραλαβής, που αναφέρει τις παρεκκλίσεις που διαπιστώθηκαν από τους όρους της σύμβασης και γνωμοδοτεί αν οι αναφερόμενες παρεκκλίσεις επηρεάζουν την καταλληλότητα των παρεχομένων υπηρεσιών και συνεπώς αν μπορούν οι τελευταίες να καλύψουν τις σχετικές ανάγκες. Στην περίπτωση αυτή εφαρμόζονται οι διατάξεις των άρθρων 219, 220 του Ν.4412/2016.

ΑΡΘΡΟ 5°

ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΣΥΜΒΑΣΗΣ

(άρθρο 216 του Ν.4412/2016)

I. Αρμόδια υπηρεσία: Η παρακολούθηση της εκτέλεσης της παρούσας σύμβασης και η διοίκηση αυτής διενεργείται από το όργανο που θα συσταθεί για το σκοπό αυτό, από την υπηρεσία του Εφετείου Αθηνών.

II. Αρμοδιότητες υπηρεσίας: Το ανωτέρω Όργανο εισηγείται στην Αναθέτουσα Αρχή για όλα τα ζητήματα που αφορούν:

- στην προσήκουσα εκτέλεση όλων των όρων της σύμβασης και στην εκπλήρωση των υποχρεώσεων της Αναδόχου εταιρίας,
- στη λήψη των επιβεβλημένων μέτρων λόγω μη τήρησης των ως άνω όρων.

ΑΡΘΡΟ 6°

ΚΗΡΥΞΗ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ ΕΚΠΤΩΤΟΥ

(άρθρο 203 του Ν.4412/2016)

Η Ανάδοχος εταιρία κηρύσσεται υποχρεωτικά έκπτωτη από την ανάθεση που έγινε στο όνομα της και από κάθε δικαίωμα που απορρέει από αυτήν :

Α) αν δεν εκπληρώσει τις συμβατικές της υποχρεώσεις ή δεν συμμορφωθεί με τις γραπτές εντολές της υπηρεσίας, που είναι σύμφωνες με την σύμβαση ή τις κείμενες διατάξεις και

Β) αν υπερβεί υπαίτια τη συνολική προθεσμία εκτέλεσης της σύμβασης, λαμβανομένων υπόψη των παρατάσεων.

Η Ανάδοχος εταιρία δεν κηρύσσεται έκπτωτη από την σύμβαση:

α) όταν με ευθύνη της Αναθέτουσας Αρχής δεν υπογράφηκε η σύμβαση ή δεν παρασχέθηκαν οι συμφωνηθείσες υπηρεσίες,

β) συντρέχουν λόγοι ανωτέρας βίας. (άρθρο 203 παρ.3 Ν.4412/16)

Αν η Ανάδοχος επικαλεστεί ανωτέρα βία υποχρεούται, μέσα σε είκοσι (20) ημέρες από τότε που συνέβησαν τα περιστατικά που συνιστούν την ανωτέρα βία, να αναφέρει εγγράφως αυτά και να προσκομίσει στην αναθέτουσα αρχή τα απαραίτητα αποδεικτικά στοιχεία. (άρθρο 204 Ν.4412/16)

Η Ανάδοχος υποχρεούται να τηρεί απαρέγκλιτα τους όρους και τις απαιτήσεις, οι οποίες αναγράφονται στην απόφαση Ανάθεσης και στην παρούσα σύμβαση. Στην αντίθετη περίπτωση θα της επιβληθούν οι κυρώσεις που προβλέπονται στα άρθρα 105§5, 203 και 218§2 α, β, γ του ν.4412/2016.

ΑΡΘΡΟ 7°

ΔΙΚΑΙΩΜΑ ΜΟΝΟΜΕΡΟΥΣ ΛΥΣΗΣ ΤΗΣ ΣΥΜΒΑΣΗΣ

(άρθρο 133 του Ν.4412/16)

Η Αναθέτουσα Αρχή μπορεί να καταγγείλει την παρούσα σύμβαση αν η Ανάδοχος δεν τηρήσει τους όρους αυτής και αν υποπέσει σε μία των προϋποθέσεων του άρθρου 133 του ν. 4412/2016.

Η Ανάδοχος υποχρεούται να τηρεί απαρέγκλιτα τους όρους και τις απαιτήσεις, οι οποίες αναγράφονται στην απόφαση Ανάθεσης και στην παρούσα σύμβαση. Στην αντίθετη περίπτωση θα της επιβληθούν οι κυρώσεις που προβλέπονται στα άρθρα 133§§1 και 2, του ν.4412/2016.

ΑΡΘΡΟ 8°

ΤΕΛΙΚΟΙ ΟΡΟΙ ΤΗΣ ΣΥΜΒΑΣΗΣ

Η παρούσα σύμβαση διέπεται από τις διατάξεις, του Ν.4412/2016. Η παρούσα σύμβαση διέπεται από την Ελληνική Νομοθεσία.

Αρμόδια για την επίλυση κάθε διαφοράς που τυχόν θα προκύψει από την εκτέλεση, εφαρμογή ή ερμηνεία της παρούσας σύμβασης είναι τα Δικαστήρια της Αθήνας. Πριν από οποιαδήποτε προσφυγή στα Δικαστήρια, σύμφωνα με τα παραπάνω, τα συμβαλλόμενα μέρη θα καταβάλλουν κάθε δυνατή προσπάθεια για φιλική διευθέτηση των διαφορών, που ενδεχομένως θα αναφύονται μεταξύ τους.

1. Απαγορεύεται η εκχώρηση, υπό οποιαδήποτε μορφή, υπό του Προμηθευτή των εκ της συμβάσεως αυτής απορρεουσών υποχρεώσεων όπως και δικαιωμάτων σε οποιονδήποτε τρίτο.
2. Σε περίπτωση ανωτέρας βίας, η απόδειξη αυτής βαρύνει εξ ολοκλήρου τον Προμηθευτή.
3. Ο Προμηθευτής θα φέρει τις απορρέουσες ευθύνες (αστικές – διοικητικές) για το προσωπικό το οποίο θα απασχολεί.
4. Κατά την εκτέλεση της σύμβασης ο προμηθευτής τηρεί τις υποχρεώσεις στους τομείς του περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, που έχουν θεσπισθεί με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές συμβάσεις ή διεθνείς διατάξεις περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α' του ν. 4412/2016 (ΦΕΚ Α' 147).
5. Σε αντικειμενικά δικαιολογημένες περιπτώσεις, εφόσον συμφωνήσουν προς τούτο και τα δύο συμβαλλόμενα μέρη, μπορεί να τροποποιείται η σύμβαση, ύστερα από γνωμοδότηση του αρμοδίου οργάνου και υπό τους όρους της κείμενης νομοθεσίας.

ΑΡΘΡΟ 9^ο **ΣΥΜΒΑΤΙΚΑ ΜΕΡΗ**

Τα στοιχεία της παρούσης σύμβασης που θα θεωρούνται ότι αποτελούν αναπόσπαστο τμήμα και θα ισχύουν με τους υπόλοιπους όρους της, είναι:

1. Το με αριθμό πρωτ. 14662/11-10-2017 Αίτημα του Εφετείου Αθηνών
2. Η από 8-02-2018 οικονομοτεχνική προσφορά της Αναδόχου εταιρίας,
3. Η 15/2018 Απόφαση Ανάθεσης του Τριμελούς Συμβουλίου Διεύθυνσης του Εφετείου Αθηνών
4. Η υπ' αριθμό πρωτ. 16682/10-11-2017 Απόφαση Ανάληψης Υποχρέωσης **(ΑΔΑ:62Κ445Τ-ΨΧΜ, ΑΔΑΜ: 17REQ002310179)**
5. Γενικές Οδηγίες Προστασίας Διαδικτυακής Υποδομής της εθνικής αρχής αντιμετώπισης ηλεκτρονικών επιθέσεων

Κατόπιν των ανωτέρω, συντάχθηκε η παρούσα σύμβαση, η οποία αφού διαβάστηκε υπογράφεται από τους συμβαλλόμενους σε τρία (3) όμοια πρωτότυπα.

ΟΙ ΣΥΜΒΑΛΛΟΜΕΝΟΙ

ΕΦΕΤΕΙΟ ΑΘΗΝΩΝ

Θεόδωρος Κανελλόπουλος,

Αρεοπαγίτης

Η ΑΝΑΔΟΧΟΣ ΕΠΙΧΕΙΡΗΣΗ

Γεώργιος Κων. Χρυσικός

ΠΑΡΑΡΤΗΜΑ

ΣΥΜΒΑΣΗΣ

ετήσιας βελτιστοποίησης-εξελικτικής συντήρησης και
φιλοξενίας της ιστοσελίδας του Εφετείου Αθηνών
(www.efeteioathinon.gr)



**Εθνική Αρχή Αντιμετώπισης
Ηλεκτρονικών Επιθέσεων**

Γενικές Οδηγίες Προστασίας Διαδικτυακής Υποδομής

Έκδοση 1.0

Φεβρουάριος 2013

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων

Εθνικό CERT

Αποστολή

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μεριμνά για την πρόληψη και τη στατική και ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής. Επιπλέον η Αρχή είναι υπεύθυνη για τη συλλογή, την επεξεργασία δεδομένων και την ενημέρωση των αρμόδιων φορέων.

Αρμοδιότητες

- Είναι η αρμόδια Εθνική Αρχή αντιμετώπισης-προστασίας από ηλεκτρονικές απειλές-επιθέσεις κυρίως προς τον Δημόσιο Φορέα και τις Κρίσιμες Υποδομές της χώρας, σύμφωνα με τον Ν. 3649/2008 και το Π.Δ. 126/2009.
- Διαθέτει το απαραίτητο επιστημονικό προσωπικό και τον απαιτούμενο εξοπλισμό για τον χειρισμό, την ανάπτυξη στρατηγικής και την αντιμετώπιση απειλών-επιθέσεων καθώς και την συλλογή, επεξεργασία και διακίνηση των σχετικών πληροφοριών.
- Για την αποτελεσματικότερη εκπλήρωση της αποστολής της, συνεργάζεται με άλλα Εθνικά και μη CERT, με τις αντίστοιχες υπηρεσίες άλλων χωρών και διεθνών οργανισμών, καθώς και Υπηρεσίες του Δημοσίου Φορέα για σχετικά θέματα.

Υπηρεσίες

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων παρέχει υπηρεσίες που άπτονται του αντικειμένου της ασφάλειας των Πληροφοριακών Συστημάτων του ευρύτερου Δημόσιου Τομέα.

Ειδικότερα, οι υπηρεσίες που παρέχονται από το Εθνικό CERT είναι οι ακόλουθες:

- Ενημέρωση του Δημόσιου φορέα για περιστατικά ασφαλείας.
- Συντονισμό των εμπλεκόμενων για την αντιμετώπιση περιστατικών ασφαλείας.
- Ανάλυση και αξιολόγηση περιστατικών ασφαλείας.
- Πρόταση των μέτρων προστασίας που απαιτούνται για εξάλειψη των επιπτώσεων από ένα περιστατικό ασφαλείας.
- Ανάλυση κακόβουλων λογισμικών.
- Διενέργεια ελέγχων ασφαλείας σε Π.Σ. του Δημόσιου τομέα.
- Έκδοση γενικών οδηγιών για την διασφάλιση των Π.Σ. του Δημόσιου τομέα.

Επικοινωνία

Για οποιοδήποτε θέμα της αρμοδιότητάς μας, μην διστάσετε να επικοινωνήσετε μαζί μας.

ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

Ε' Διεύθυνση / 4ο τμήμα - ΕΘΝΙΚΗ ΑΡΧΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΘΕΣΕΩΝ

Ταχ. Δ/νση: Π. Κανελλοπούλου 4, Αθήνα 10177

Τηλ.: 210 6973541 – Fax: 210 6923239

Email: cert@nis.gr – Web: www.cert.gov.gr

Περιεχόμενα

A. Εισαγωγή	4
B. Γενικά μέτρα προστασίας διαδικτυακού διακομιστή	4
Γ. Γενικά μέτρα προστασίας ιστοτόπου	5
Δ. Μέτρα προστασίας ιστοτόπου «Joomla».....	7
Ε. Μέτρα προστασίας ιστοτόπου «Wordpress»	9
ΣΤ. Ενέργειες αντιμετώπισης επίθεσης	11
Ζ. Βιβλιογραφία.....	11

A. Εισαγωγή

Ο βασικός κανόνας για την διασφάλιση ενός διαδικτυακού πληροφοριακού συστήματος είναι η διαρκής ενημέρωση στην τελευταία έκδοση και η διαρκής εποπτεία του μέσω της παρακολούθησης του συνόλου των Log Files, των ελεγκτικών πολιτικών (auditing), των υπηρεσιών του, των αρχείων του και της δικτυακής συμπεριφοράς του.

Θα πρέπει να λαμβάνεται υπόψη ότι κανένα λογισμικό δεν είναι απόλυτα ασφαλές.

Οι πλατφόρμες λογισμικού ανοικτού κώδικα (Joomla, Wordpress κ.α.) αναπτύσσονται και υποστηρίζονται από ομάδες προγραμματιστών μη πιστοποιημένων και δεν παρέχονται εγγυήσεις για το επίπεδο υπηρεσιών του τελικού προϊόντος. Επιπλέον η διάθεση του πηγαίου κώδικα στο ευρύ κοινό συνιστά μειονέκτημα ασφαλείας καθώς ο οποιοσδήποτε δύναται να εντοπίσει κενό ασφαλείας και να το εκμεταλλευτεί κακόβουλα. Κενά ασφαλείας και οδηγίες εκμετάλλευσης τους είναι διαθέσιμες, χωρίς κόστος, στο διαδίκτυο αυξάνοντας σημαντικά το ρίσκο επιτυχημένης ηλεκτρονικής επίθεσης ακόμα και από αρχάριους χρήστες.

Στις πλατφόρμες λογισμικού ανοικτού κώδικα δεν παρέχεται καμία εγγύηση ασφάλειας από τους προγραμματιστές που τις αναπτύσσουν. Το έργο της διασφάλισης και της προστασίας του ιστοτόπου από ηλεκτρονικές επιθέσεων, εναπόκειται στον διαχειριστή και στον υπεύθυνο ασφαλείας του.

Το παρόν έγγραφο περιλαμβάνει οδηγίες για το πώς να μπορεί να γίνει μία διαδικτυακή υποδομή ασφαλέστερη (hardening).

B. Γενικά μέτρα προστασίας διαδικτυακού διακομιστή

1) Εγκατάσταση του λειτουργικού συστήματος σε μεμονωμένο διακομιστή ή σε μεμονωμένο εικονικό περιβάλλον (Guest OS).

2) Ενημέρωση των εγκατεστημένων λογισμικών στην τελευταία έκδοση.

3) Εγκατάσταση και ενημέρωση αντιϊικού λογισμικού.

4) Δημιουργίας ρουτίνας (script job) που θα επιτηρεί και θα αναφέρει οποιαδήποτε μεταβολή των αρχείων του διακομιστή στον διαχειριστή. Οι ρουτίνες μπορούν να υλοποιηθούν είτε μέσω Cron είτε μέσω Windows task scheduler.

5) Το περιεχόμενο του ιστοτόπου θα πρέπει να εγκατασταθεί σε διαφορετικό σκληρό δίσκο από αυτόν που εγκαταστάθηκε το Λειτουργικό Σύστημα.

6) Απενεργοποίηση των υπηρεσιών που δεν χρειάζονται για την λειτουργία του ιστότοπου.

7) Κατάργηση των λογαριασμών χρηστών που δεν χρειάζονται για την λειτουργία του ιστότοπου.

8) Οι κωδικοί χρηστών θα πρέπει να τηρούν κανόνες πολυπλοκότητας και να αλλάζουν υποχρεωτικά σε τακτά χρονικά διαστήματα.

9) Οι ρόλοι με δικαιώματα διαχειριστή και υπεύθυνου ασφαλείας του διακομιστή θα πρέπει να αντιστοιχούν σε φυσικά πρόσωπα που ανήκουν στο ανθρώπινο δυναμικό του φορέα.

10) Διαγραφή όλων των αρχείων δοκιμών (test files).

11) Μεταβολή του HTTP banner του διακομιστή ώστε να αποκρύπτει τον τύπο και την έκδοση του Λειτουργικού Συστήματος.

12) Εγκατάσταση του διαδικτυακού διακομιστή σε DMZ.

13) Στην DMZ είναι θεμιτό να εγκατασταθεί IDS/IPS για την προστασία του διαδικτυακού διακομιστή. Χρήση δικτυακών συσκευών που θα προστατεύουν από δικτυακές επιθέσεις (π.χ. port scan).

14) Παραμετροποίηση του διακομιστή ώστε να καταγράφει πλήρη Logs και να τα αποθηκεύει σε ξεχωριστό υπολογιστή για τουλάχιστον 12 μήνες.

15) Τα Logs θα πρέπει να καταγράφουν την IP και την Port του επισκέπτη που εκτελεί αίτημα στον διακομιστή ακόμα και στην περίπτωση που μεσολαβεί Proxy Server. Για παράδειγμα στον Apache θα πρέπει να οριστεί το πεδίο `%{remote}p`. Στον IIS η ρύθμιση γίνεται μόνο στην έκδοση από IIS7.5 και πάνω με το πρόσθετο «Advance Logging». Θα πρέπει να οριστεί στις παραμέτρους ένα νέο πεδίο (ID=) «c-port» του τύπου (Source Type=) «Server Variable» και όνομα (Source Name=) «REMOTE_PORT».

16) Η ημερομηνία και η ώρα των Logs να είναι συγχρονισμένη σε GMT.

17) Απαραίτητο για τον έλεγχο της καλής λειτουργίας του διακομιστή είναι η εφαρμογή ελεγκτικής πολιτικής (auditing). Θα πρέπει κάθε ενέργεια χρήστη, που μεταβάλει δεδομένα και ρυθμίσεις στον διακομιστή, να καταγράφεται.

18) Ορισμός υπεύθυνων διαχείρισης και ασφαλείας, όπου με έγγραφο θα καθορίζονται οι αρμοδιότητες τους και τα καθήκοντα τους.

19) Καταγραφή σε έγγραφο όλων των εγκατεστημένων λογισμικών και των ρυθμίσεων τους. Η καταγραφή θα είναι το πλήρες ιστορικό του διακομιστή. Πιο συγκεκριμένα θα πρέπει να καταγράφονται η ημερομηνία εγκατάστασης λογισμικού, η έκδοση του, ο σκοπός λειτουργίας του και τις αναβαθμίσεις.

Γ. Γενικά μέτρα προστασίας ιστοτόπου

1) Εγκατάσταση του ιστοτόπου και της βάσης δεδομένων του, αν υπάρχει, σε διαφορετικούς διακομιστές. Η σύνδεση τους θα πρέπει να προστατεύεται από τείχος προστασίας (Firewall) όπου θα επιτρέπεται η επικοινωνία μόνο στις απαραίτητες θύρες για την επικοινωνία site και DBMS.

2) Οι χρήστες του ιστοτόπου και της βάσης δεδομένων, δεν θα πρέπει να αντιστοιχούν σε χρήστες του λειτουργικού συστήματος των διακομιστών που τα φιλοξενεί. Για παράδειγμα σε εγκατάσταση Ms SQL Server η διασύνδεση με τον ιστότοπο θα πρέπει να γίνεται μόνο με χρήστη δηλωμένο στο DBMS (SQL Server user, όχι windows authentication) και παραμετροποιημένα δικαιώματα αποκλειστικά για την υλοποίηση του ADODB (όχι SA στο DBMS).

3) Η πλατφόρμα υποστήριξης του ιστοτόπου και η βάση δεδομένων θα πρέπει να είναι ενημερωμένες πλήρως στην τελευταία τους έκδοση. Για παράδειγμα, αν το site είναι Wordpress και η βάση δεδομένων MySQL τότε θα πρέπει να είναι στην τελευταία τους έκδοση.

4) Η πληροφορία που χρησιμοποιείται στις εφαρμογές αυτές πρέπει να προστατεύεται από μη επιτρεπτή αποκάλυψη ή αλλοίωση με τον έλεγχο των δεδομένων εισόδου σε επίπεδο χρήστη.

5) Τα ευαίσθητα δεδομένα, αν υπάρχουν, θα πρέπει να αποθηκεύονται κρυπτογραφημένα. Για παράδειγμα οι κωδικοί πρόσβασης θα πρέπει να είναι κρυπτογραφημένοι στην βάση δεδομένων.

6) Οι τοποθεσίες που περιέχουν αρχεία θα πρέπει να προστατεύονται με περιορισμένη πρόσβαση και περιορισμένα δικαιώματα.

7) Ο κώδικας του ιστοτόπου θα πρέπει να προστατεύει τον ιστότοπο από τις ακόλουθες διαδικτυακές επιθέσεις, όπως έχουν καταγραφεί από τον OWASP:

- A1 – Injection
- A2 – Cross Site Scripting /XSS
- A3 – Broken Authentication / Session Management
- A4 – Insecure Direct Object References
- A5 – Cross Site Request Forgery
- A6 – Security Misconfiguration
- A7 – Insecure Cryptographic Storage
- A8 – Failure to Restrict URL Access
- A9 – Insufficient Transport Layer Protection
- A10 – Unvalidated Redirects and Forwards

8) Σε κάθε σελίδα Login διαχείρισης περιεχομένου και παραμετροποίησης του ιστοτόπου θα πρέπει να χρησιμοποιείται SSL και η πρόσβαση να επιτρέπεται μόνο από συγκεκριμένες IP (εσωτερικού δικτύου). Όπου απαιτείται απομακρυσμένη πρόσβαση συνίσταται η δημιουργία σύνδεσης VPN προς το εσωτερικό δίκτυο.

9) Οι κωδικοί χρηστών θα πρέπει να τηρούν κανόνες πολυπλοκότητας και να αλλάζουν υποχρεωτικά σε τακτά χρονικά διαστήματα.

10) Απενεργοποίηση των symbolic links.

11) Χρήση του robots.txt με τις ακόλουθες ρυθμίσεις:

- User-agent: *
- Disallow: /images/
- Disallow: /banners/
- Disallow: /Forms/
- Disallow: /Dictionary/
- Disallow: /_borders/
- Disallow: /_fpclass/
- Disallow: /_overlay/
- Disallow: /_private/
- Disallow: /_themes/

- κ.λ.π. κατά την κρίση σας

12) Απαραίτητο για τον έλεγχο της καλής λειτουργίας του ιστότοπου, αλλά και γενικότερα κάθε λογισμικού, είναι η εφαρμογή ελεγκτικής πολιτικής (auditing). Θα πρέπει κάθε ενέργεια χρήστη που μεταβάλλει δεδομένα, ρυθμίσεις στον ιστότοπο και την υποδομή του να καταγράφεται.

13) Ορισμός υπεύθυνων διαχείρισης ιστοτόπου, διαχείρισης περιεχομένου και ασφαλείας, όπου με έγγραφο θα καθορίζονται οι αρμοδιότητες τους και τα καθήκοντα τους. Οι χρήστες με ρόλους αυξημένων δικαιωμάτων θα πρέπει να είναι συγκεκριμένοι (όχι περισσότεροι από δύο για κάθε ρόλο) και να αντιστοιχούν σε φυσικά πρόσωπα που ανήκουν στο ανθρώπινο δυναμικό του φορέα.

14) Καταγραφή σε έγγραφο όλων των επιμέρους ρυθμίσεων του ιστοτόπου και της βάσης δεδομένων του. Η καταγραφή θα είναι το πλήρες ιστορικό του κυρίως ιστοτόπου και των πρόσθετων του. Πιο συγκεκριμένα θα πρέπει να καταγράφονται η ημερομηνία αρχικής εγκατάστασης, η ημερομηνία εγκατάστασης αναβαθμίσεων, η έκδοση του λογισμικού και ο σκοπός λειτουργίας του.

Δ. Μέτρα προστασίας ιστοτόπου «Joomla»

1) Εγκατάσταση της τελευταίας επίσημης έκδοσης του Joomla. Θα πρέπει πριν την εγκατάσταση της να λαμβάνεται backup του site. Οποσδήποτε να ελέγχεται μέσω του MD5 ότι κατέβηκε η σωστή έκδοση.

2) Αλλαγή του ονόματος διαχειριστή, από admin σε οτιδήποτε επιθυμείτε αλλά καλό θα ήταν να μην είναι εύκολα προβλέψιμο.

3) Επιλογή πολύπλοκου κωδικού πρόσβασης και συχνή αλλαγή του.

4) Προστασία του αρχείου ρυθμίσεων configuration.php καθώς και οποιοδήποτε φακέλου που σχετίζεται με ρυθμίσεις (π.χ. extension) θα πρέπει να βρίσκεται εκτός φακέλου public_html.

5) Οι φάκελοι που περιέχουν Logs θα πρέπει να προστατεύονται με http authentication.

6) Οι φάκελοι logs και temp θα πρέπει να είναι εντός της ρύθμισης base_dir.

7) Επιλογή δικαιωμάτων πρόσβασης (τα ακριβή δικαιώματα εξαρτώνται από την υλοποίηση του hosting provider):

- Για τα αρχεία *.php τα δικαιώματα να είναι 644 (rw- r-- r--).
- Για τα υπόλοιπα τα δικαιώματα να είναι 755 (rwx r-x r-x).
- Ειδικά για τους φακέλους /images/ και /images/stories/ τα δικαιώματα μπορεί να είναι 707 (rwx --- rwx).

8) Σε κάθε σελίδα Login θα πρέπει να χρησιμοποιείται SSL και η πρόσβαση να περιορίζεται σε συγκεκριμένες IP (εσωτερικού δικτύου) για την προστασία κάθε οθόνης εισόδου στο site (π.χ. /administrator/). Ο περιορισμός θα πρέπει να επεκτείνεται και στους χρήστες που θα έχουν δικαιώματα συντήρησης.

9) Ενεργοποίηση του αρχείου .htaccess (και διαγραφή του htaccess.txt) τοποθετώντας το στο root directory του site. Το .htaccess θα πρέπει να περιέχει

```

### Begin - Rewrite rules to block out some common exploits
# Prevent use of specified methods in HTTP Request
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK) [NC,OR]
# Block out use of illegal or unsafe characters in the HTTP Request
RewriteCond %{THE_REQUEST} ^.*(\r|\n|%0A|%0D).* [NC,OR]
# Block out use of illegal or unsafe characters in the Referer Variable of the HTTP Request
RewriteCond %{HTTP_REFERER} ^(.*)(<|>|'|"%0A|%0D|%27|%3C|%3E|%00).* [NC,OR]
# Block out use of illegal or unsafe characters in any cookie associated with the HTTP Request
RewriteCond %{HTTP_COOKIE} ^.*(<|>|'|"%0A|%0D|%27|%3C|%3E|%00).* [NC,OR]
# Block out use of illegal characters in URI or use of malformed URI
RewriteCond %{REQUEST_URI} ^(/,|:|;|<|>|'|">|"/\\\\.\\.\\.\\.){0,9999}.* [NC,OR]
# NOTE - disable this rule if your site is integrated with Payment Gateways such as PayPal
# Block out use of empty User Agent Strings
RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
# Block out use of User Agent Strings beginning with java, curl or wget
RewriteCond %{HTTP_USER_AGENT} ^(java|curl|wget).* [NC,OR]
# Block out use of User Agent Strings containing specific robot (crawler) identifiers
RewriteCond %{HTTP_USER_AGENT}
^.*(winhttp|HTTrack|clshttp|archiver|loader|email|harvest|extract|grab|miner).* [NC,OR]
# Block out use of User Agent Strings containing references to specific crawler libraries
RewriteCond %{HTTP_USER_AGENT} ^.*(libwww-perl|curl|wget|python|nikto|scan).* [NC,OR]
# Block out use of illegal or unsafe characters in the User Agent variable
RewriteCond %{HTTP_USER_AGENT} ^.*(<|>|'|"%0A|%0D|%27|%3C|%3E|%00).* [NC,OR]
# Measures to block out SQL injection attacks
RewriteCond %{QUERY_STRING}
^.*(;|<|>|'|"\\)|%0A|%0D|%22|%27|%3C|%3E|%00).*(^/*|union|select|insert|cast|set|declare|drop|update|
md5|benchmark).* [NC,OR]
# Block out reference to localhost/loopback/127.0.0.1 in the Query String
RewriteCond %{QUERY_STRING} ^.*(localhost|loopback|127\\.0\\.0\\.1).* [NC,OR]
# Block out use of illegal or unsafe characters in the Query String variable
RewriteCond %{QUERY_STRING} ^.*(<|>|'|"%0A|%0D|%27|%3C|%3E|%00).* [NC]
#### End of commented Rewrite directives
####Protect sensitive files
<FilesMatch "\.(htaccess|htpasswd|ini|phps|log|sh|conf)$">
Order allow,deny
Deny from all
</FilesMatch>
<FilesMatch "configuration.php">
Order allow,deny
Deny from all
</FilesMatch>

```

- Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων

- Δεν έχει εγκαταλειφθεί η υποστήριξη του από την ομάδα ανάπτυξης.
 - Η έκδοση του πρόσθετου έχει τη σήμανση «σταθερή» (stable και όχι beta κ.τ.λ.).
 - Ο πηγαίος κώδικας του πρόσθετου δεν είναι κωδικοποιημένος.
 - Αποφεύγετε πρόσθετα που σαν λειτουργία παρέχουν την δυνατότητα εγγραφής – μεταβολής αρχείων στο site.
 - Αποφεύγεται πρόσθετα που επιτρέπουν την αυτόματη εγγραφή χρηστών στο site ακόμα και σε επίπεδο user. Κάθε εγγραφή χρήστη θα πρέπει να εγκρίνεται από τον διαχειριστή του ιστοτόπου.
- 12) Κατά την απεγκατάσταση ενός πρόσθετου βεβαιωθείτε ότι διαγράφετε όλα τα αρχεία που αναφέρονται στο xml του πρόσθετου.
- 13) Απενεργοποίηση του Directory Browsing.
- 14) Θα πρέπει να μην υπάρχουν υπολείμματα αρχείων στον διακομιστή. Μία αποτυχημένη εγκατάσταση/απεγκατάσταση ενός πρόσθετου μπορεί να αποτελέσει πιθανή τρωτότητα σε κάποια επίθεση. Η συνήθης διαδρομή υπολειμμάτων είναι /tmp/directory.

Ε. Μέτρα προστασίας ιστοτόπου «Wordpress»

- 1) Εγκατάσταση της τελευταίας επίσημης έκδοσης του Wordpress. Θα πρέπει πριν την εγκατάσταση της να λαμβάνεται backup του site για λόγους συμβατότητας. Οποσδήποτε να ελέγχεται μέσω του MD5 ότι κατέβηκε η σωστή έκδοση. Μην χρησιμοποιείτε αυτόματη ενημέρωση, πάντα να γίνεται ελεγχόμενα από τον διαχειριστή.
- 2) Αλλαγή του ονόματος διαχειριστή σε οτιδήποτε επιθυμείτε αλλά καλό θα ήταν να μην είναι εύκολα προβλέψιμο. Γενικά δεν θα πρέπει να υπάρχει χρήστης με όνομα admin.
- 3) Επιλογή πολύπλοκου κωδικού πρόσβασης και συχνή αλλαγή του.
- 4) Αλλαγή του προθέματος wp_ στην βάση δεδομένων.
- 5) Διαγραφή της έκδοσης Wordpress από τον header. Η αλλαγή γίνεται μέσω του πηγαίου κώδικα με την γραμμή `<?php remove_action('wp_head', 'wp_generator'); ?>` . Διαγραφή του Readme.txt.
- 6) Επιλογή δικαιωμάτων πρόσβασης (τα ακριβή δικαιώματα εξαρτώνται από την υλοποίηση του hosting provider):
- Για τα αρχεία *.php τα δικαιώματα να είναι 644 (rw- r-- r--).
 - Για τους φακέλους τα δικαιώματα να είναι 755 ().
 - Στο root directory(/), /wp-admin/, /wp-includes/, /wp-content/plugins/ θα πρέπει να έχει πρόσβαση μόνο ο χρήστης με δικαιώματα διαχειριστή. Αυτό συνεπάγεται προστασία των directories με κωδικό.

- Το .htaccess θα πρέπει να προσπελάζεται και από το web server service. Το ίδιο θα πρέπει να ισχύει και για τα /wp-content/ και /wp-content/themes/.

7) Κάθε οθόνη εισόδου θα πρέπει να προστατεύεται από SSL και η πρόσβαση σε διαχειριστές να περιορίζεται σε συγκεκριμένες IP (εσωτερικού δικτύου) για την προστασία κάθε οθόνης εισόδου στο site. Ο περιορισμός θα πρέπει να επεκτείνεται και στους χρήστες που θα έχουν δικαιώματα συντήρησης περιεχομένου.

8) Προστασία κάθε αρχείου που σχετίζεται με ρυθμίσεις (π.χ. httpsswds) θα πρέπει να βρίσκεται εκτός φακέλου public_html.

9) Προστασία του φακέλου /wp-includes/ με .htaccess που θα έχει τις ακόλουθες εντολές:

```
# Block the include-only files.
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^\.]+\.\php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
```

10) Απενεργοποίηση του δικαιώματος αλλαγής πηγαίου κώδικα. Η αλλαγή γίνεται μέσω του πηγαίου κώδικα με την γραμμή `define('DISALLOW_FILE_EDIT', true);`

11) Πριν την εγκατάσταση ενός πρόσθετου σιγουρευτείτε για τα ακόλουθα:

- Το πρόσθετο δεν έχει γνωστά κενά ασφαλείας που δεν έχουν διορθωθεί.
- Δεν έχει εγκαταλειφθεί η υποστήριξη του από την ομάδα ανάπτυξης.
- Η έκδοση του πρόσθετου έχει τη σήμανση «σταθερή» (stable και όχι beta κ.τ.λ.).
- Ο πηγαίος κώδικας του πρόσθετου δεν είναι κωδικοποιημένος.
- Αποφεύγετε πρόσθετα που σαν λειτουργία παρέχουν την δυνατότητα εγγραφής – μεταβολής αρχείων στο site.
- Αποφεύγετε πρόσθετα που επιτρέπουν την αυτόματη εγγραφή χρηστών στο site ακόμα και σε επίπεδο user. Κάθε εγγραφή χρήστη θα πρέπει να εγκρίνεται από τον διαχειριστή του ιστοτόπου. Το ίδιο θα πρέπει να γίνεται και για την ανάρτηση σχολίων από χρήστες.

12) Κατά την απεγκατάσταση ενός πρόσθετου βεβαιωθείτε ότι διαγράφετε όλα τα αρχεία που αναφέρονται στο xml του πρόσθετου.

13) Θα πρέπει να μην υπάρχουν υπολείμματα αρχείων στον διακομιστή. Μία αποτυχημένη εγκατάσταση/απεγκατάσταση ενός πρόσθετου μπορεί να αποτελέσει πιθανή τρωτότητα σε κάποια επίθεση.

14) Απενεργοποίηση του Directory Browsing.

ΣΤ. Ενέργειες αντιμετώπισης επίθεσης

- 1) Ενημέρωση του Hosting Provider, του Εθνικού CERT και του εποπτεύοντα φορέα.
- 2) Ο ιστότοπος να τεθεί εκτός λειτουργίας (Offline).
- 3) Συλλογή στοιχείων για το περιστατικό:
 - Δημιουργία Image των σκληρών δίσκων των διακομιστών (του ιστοτόπου και της βάσης δεδομένων) σε διαμόρφωση bit-bit.
 - Συλλογή των αρχείων που πιθανώς ανήρτησαν οι επιτιθέμενοι.
 - Συλλογή των Log Files του διακομιστή.
 - Συλλογή των Log Files των εγκατεστημένων λογισμικών.
 - Συλλογή των Log Files του ιστοτόπου.
 - Αποστολή των ανωτέρω δεδομένων στο Εθνικό CERT για ανάλυση.
- 4) Επανεγκατάσταση της υποδομής.
 - Διαμόρφωση διακομιστή και επανεγκατάσταση του λειτουργικού συστήματος και των δευτερευόντων προγραμμάτων, ώστε να διασφαλιστεί ότι δεν έχουν μείνει υπολείμματα από την επίθεση.
 - Εφαρμογή των μέτρων που αναλύονται στις §Β και §Γ του παρόντος.
 - Ενδελεχής έλεγχος του τελευταίου διαθέσιμου BackUp του περιεχομένου του ιστοτόπου ώστε να διαπιστωθεί ότι είναι ασφαλές.
 - Επαναφορά του τελευταίου «καθαρού» διαθέσιμου BackUp του περιεχομένου του ιστοτόπου. Οι ρυθμίσεις θα πρέπει να γίνουν από την αρχή.
 - Αλλαγή των κωδικών πρόσβασης των χρηστών.
 - Εφαρμογή εξειδικευμένων μέτρων κατά περίπτωση σε συνεργασία με το Εθνικό CERT.

Z. Βιβλιογραφία

- <http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>
- <http://www.nis.gr/npimages/docs/Genika%20Metra%20Prostasias%20Cert.pdf>
- http://docs.joomla.org/Security_Checklist/Joomla!_Setup
- http://docs.joomla.org/Security_Checklist/You_have_been_hacked_or_defaced
- http://docs.joomla.org/Security_and_Performance_FAQs
- <http://developer.joomla.org/security.html>
- http://docs.joomla.org/Top_10_Stupidest_Administrator_Tricks
- http://bodvoc.com/index.php?option=com_content&view=article&id=43:improving-your-joomla-htaccess-file&catid=2:joomla-security&itemid=3
- <http://wp.tutsplus.com/tutorials/10-steps-to-securing-your-wordpress-installation/>

- http://codex.wordpress.org/Hardening_WordPress
- <http://kuttler.eu/post/htaccess-protect-wordpress-admin/>
- https://www.owasp.org/index.php/Main_Page