Σύνταξη:	01.06.2021	Νικόλαος Βορδώνης		**Έγκριση**:	01.06.2021	Ζαφειρόπουλος Χαράλαμπος	
	Ημερομηνία,	Ονοματεπώνυμο,	Υπογραφή		Ημερομηνία,	Ονοματεπώνυμο,	Υπογραφή

ΑΝΤΙΓΡΑΦΟ: ☐ ΕΛΕΓΧΟΜΕΝΟ ☐ ΜΗ ΕΛΕΓΧΟΜΕΝΟ

ΠΙΝΑΚΑΣ ΜΕΤΑΒΟΛΩΝ

Α/Α	*ΗΜΕΡΟΜΗΝΙΑ*	*ΠΕΡΙΓΡΑΦΗ ΑΝΑΘΕΩΡΗΣΗΣ*	*ΕΔΑΦΙΟ*	*ΣΥΝΤΑΞΗ*	*ΕΓΚΡΙΣΗ*
01	**10.04.2019**	**Αρχική Έκδοση Σύμφωνα με απαιτήσεις ISO 27001:2013**			
02	**01.06.2021**	**Εισαγωγή Πολιτικής Τηλεεργασίας**			
03					
04					
05					
06					
07					
08					
09					
10					

ΣΚΟΠΟΣ

Η ΑΠΟΨΗ ΑΕ, εφεξής "Εταιρία", ως διακεκριμένος Φορέας παροχής υπηρεσιών εκπαίδευσης, αποδίδει μεγάλη σημασία στην σύννομη επεξεργασία, ασφάλεια και προστασία των προσωπικών δεδομένων, υπό οποιαδήποτε ιδιότητα συνεργασίας ή επικοινωνίας (όπως, ενδεικτικά, οι υποψήφιοι ή ενεργοί Πελάτες, Συνεργάτες, Εκπαιδευόμενοι, Προμηθευτές, Εργαζόμενοι, Ιδιώτες, επισκέπτες ιστοσελίδων ή γενικά συνεργαζόμενοι τρίτοι με τον Οργανισμό της).

Η ΑΠΟΨΗ ΑΕ στοχεύει στην απρόσκοπτη παροχή υπηρεσιών υψηλής ποιότητας στην τοπική κοινότητα χρηστών, στο να επιτύχει τους επιχειρηματικούς στόχους και αποστολή της, προστατεύοντας τους φυσικούς και οικονομικούς πόρους της, την εταιρική φήμη της, την νομική θέση της, τους υπαλλήλους της, και όλα τα υπόλοιπα ενσώματα και άυλα περιουσιακά στοιχεία της, όπως απαιτούνται από την Αρχή Προστασίας Προσωπικών Δεδομένων και της Αρχής Διασφάλισης των Προσωπικών Δεδομένων αλλά και από τις απαιτήσεις του προτύπου ISO 27001:2013.

Η Διοίκηση της ΑΠΟΨΗ ΑΕ πιστεύει ότι απαιτείται συνεχής βελτίωση του επιπέδου ασφαλείας των πληροφοριών που η εταιρεία διαχειρίζεται, ώστε η ποιότητα των επιχειρησιακών δραστηριοτήτων να παραμένει διαρκώς σε ανταγωνιστικό επίπεδο και η εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας - με στοιχεία που επιτρέπουν την αυτοαξιολόγηση και βελτίωσή του – αποτελεί στρατηγική επιλογή της με σκοπό την επίτευξη αυτού του στόχου.
Για το λόγο αυτό, η Διοίκηση αφενός δεσμεύεται στην υλοποίηση της Πολιτικής Ασφάλειας που εκφράζεται στη παρούσα και αφετέρου υποστηρίζει έμπρακτα το προσωπικό για την ενεργή συμμετοχή του στην προσπάθεια αυτή.

ΟΡΙΣΜΟΙ / ΣΥΝΤΟΜΕΥΣΕΙΣ

ΥΔΑΠ	Υπεύθυνος Διαχείρισης Ασφάλειας Πληροφοριών
ΠΤ	Προϊστάμενος Τεχνικού
ΥΠΣ	Υπεύθυνος Πληροφοριακών Συστημάτων
ΣΔΑΠ	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
ΔΣ	Διευθύνων Σύμβουλος

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Όσα ορίζονται στο παρόν κείμενο εφαρμόζονται σε όλα τα Έγγραφα του ΣΔΑΠ, δηλαδή:

- Τις Πολιτικές Ασφάλειας
- Το Πεδίο Εφαρμογής του Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών
- Στις Διαδικασίες Διαχείρισης της Ασφάλειας.
- Στις Οδηγίες Εργασίας (Προδιαγραφές, Οδηγίες Επιθεωρήσεων, Οδηγίες Συντήρησης Εξοπλισμού, κ.λ.π).

- Σε άλλα Έγγραφα Εσωτερικής ή Εξωτερικής Προέλευσης, τα οποία επηρεάζουν άμεσα ή έμμεσα την ασφάλεια των πληροφοριών που η επιχείρηση διαχειρίζεται.

ΕΦΑΡΜΟΓΗ

Ενέργειες

α/α	Εφαρμογή
1	Στα πλαίσια των ανωτέρω η Διοίκηση έχει ορίσει υπεύθυνο στέλεχος της που συνεργάζεται στενά με την ΑΠΟΨΗ ΑΕ, εφαρμόζοντας τη παρούσα Πολιτική σε όλο το εύρος της εταιρείας, φροντίζοντας για την εφαρμογή της και παράλληλα ελέγχοντας για την αποτελεσματικότητά της. • Η ενημέρωση του προσωπικού αξιολογείται τακτικά. Τα συμβάντα ασφάλειας αναγνωρίζονται έγκαιρα και λαμβάνονται αντίστοιχες διορθωτικές ενέργειες. • Οι αδυναμίες του περιβάλλοντος της εταιρείας αξιολογούνται τακτικά. • Τα συστήματα πληροφορικής και επικοινωνιών της εταιρείας ελέγχονται για να είναι πάντα στις τελευταίες ενημερωμένες εκδόσεις λογισμικού. • Το προσωπικό είναι ενημερωμένο και έχει επαρκείς δεξιότητες σε θέματα ΗΥ. • Έχει αναπτυχθεί και εφαρμοστεί Πολιτική που απαιτεί ισχυρά passwords για όλους τους χρήστες. • Η επίδοση των συστημάτων και των δικτύων παρακολουθείται συνεχώς. • Τα αρχεία καταγραφής (logs) που δημιουργούνται σε λειτουργικά συστήματα, εφαρμογές και συστήματα δικτύου ελέγχονται τακτικά. • Οι διαδικασίες back-up & restore επανελέγχονται σε τακτά χρονικά διαστήματα από το τμήμα IT της ΑΠΟΨΗ ΑΕ. • Έχει δημιουργηθεί μηχανισμός «ανταπόκρισης σε συμβάντα ασφάλειας» με σαφή καθήκοντα και διαδικασίες. • Σε κάθε περίπτωση, λαμβάνοντας υπόψη τη φύση των εργασιών της εταιρίας και των δεδομένων και πληροφοριών που διαχειρίζεται (όχι ευαίσθητα, όχι προσωπικά) η Πολιτική Ασφαλείας της εταιρίας υπερκαλύπτει τις επιχειρησιακές και νομικές ανάγκες.

Αναθεώρηση της Πολιτικής Ασφάλειας Πληροφοριών

α/α	Εφαρμογή
1	Η Πολιτική Ασφάλειας αποτελεί ακρογωνιαίο λίθο του Συστήματος Ασφάλειας Πληροφοριών. Ως εκ τούτου θα επανεξετάζεται τακτικά (μία φορά το χρόνο) για τυχόν νέους κινδύνους/απειλές ή σε περιπτώσεις σημαντικών αλλαγών της πληροφοριακής υποδομής.

Πολιτική 1. Backup

α/α	Εφαρμογή
1	Από την ΑΠΟΨΗ ΑΕ το backup εκτελείται καθημερινά μέσω ανάλογου λειτουργικού. Στα παραγωγικά συστήματα παίρνεται image και αρχεία – εβδομαδιαία.

Πολιτική 2. Συμμόρφωση προς Ισχύοντα Πρότυπα και Κανονισμούς

α/α	Εφαρμογή
1	Η Εταιρεία λαμβάνει υπόψη της τα ισχύοντα πρότυπα, τη νομοθεσία, τους κανονισμούς καθώς και τις οδηγίες εφαρμογής τους σε όλες τις επιχειρηματικές δράσεις που δραστηριοποιείται. Εφόσον αυτό είναι απαραίτητο, πιστοποιεί την συμμόρφωσή της προς τα παραπάνω μέσω πιστοποιητικών που λαμβάνει από Δημόσιους ή διαπιστευμένους προς αυτόν τον σκοπό φορείς.

Πολιτική 3. Ανταλλαγής Πληροφοριών

α/α	Εφαρμογή
1	Απαγορεύεται η ανταλλαγή ευαίσθητων δεδομένων μέσω email εκτός της εταιρείας. Σαν ευαίσθητα δεδομένα συμπεριλαμβάνονται, τα δεδομένα πελατών της εταιρείας, οικονομικά στοιχεία και στοιχεία εμπορικής στρατηγικής.

Πολιτική 4. Μητρώο Περιουσιακών Στοιχείων IT

α/α	Εφαρμογή
1	Τα περιουσιακά στοιχεία πληροφορικής θα βρίσκονται καταγεγραμμένα σε ένα η περισσότερα μητρώα. Κάθε μητρώο θα έχει έναν υπεύθυνο ιδιοκτήτη ο οποίος θα επιτελεί τον ρόλο του «Υπεύθυνου Μητρώου».

Πολιτική 5. Ασφάλεια Φυσικής Πρόσβασης

α/α	Εφαρμογή
1	Η πρόσβαση στο κτήριο της εταιρείας είναι ελεγχόμενη και επιτηρούμενη (κάμερες, κάρτες, ηλεκτρονικές κλειδαριές). Όλοι οι επισκέπτες καταγράφονται κατά την είσοδό τους στις εγκαταστάσεις της

α/α	Εφαρμογή
	εταιρείας και συνοδεύονται πάντα από εγκεκριμένο προς τούτο εκπρόσωπο του προσωπικού της εταιρείας. Η εκφόρτωση αναλωσίμων η άλλων ειδών θα γίνεται σε επιτηρούμενους και επιτρεπόμενους χώρους πάντα με συνοδεία του αρμόδιου προσωπικού της εταιρείας μας. Κατά τις μη εργάσιμες ώρες και ημέρες (καθημερινά από τις 21:00 - 08:00, Σαββατοκύριακα και αργίες) το κτίριο παραμένει κλειδωμένο.

Πολιτική 6. Risk Management

α/α	Εφαρμογή
1	Η προστασία των περιουσιακών στοιχείων που θα βρίσκονται καταγεγραμμένα στα μητρώα θα βασίζεται σε αποτίμηση των αδυναμιών τους και των κινδύνων που τα απειλούν. Η αποτίμηση των κινδύνων λαμβάνει υπόψη : • Την συμβολή κάθε στοιχείου στην αποστολή της εταιρείας • Τις αδυναμίες • Τους κινδύνους • Τις επιπτώσεις από ενδεχόμενη προσβολή • Μοναδικά σημεία αστοχίας • Μέθοδο ποσοτικοποίησης και αποτίμησης των κινδύνων • Τρόπους μείωσης των επιπτώσεων μέσω εφαρμογής μέτρων προστασίας. Η διαχείριση κινδύνων ακολουθεί συγκεκριμένη μεθοδολογία και έχει ως αποτέλεσμα ένα «Σχέδιο Αντιμετώπισης Κινδύνων», το οποίο αναθεωρείται σε τακτά χρονικά διαστήματα.

Πολιτική 7. Διαρροή Πληροφοριών

α/α	Εφαρμογή
1	Οσοι εργάζονται σε διαβαθμισμένα έργα φροντίζουν να μην μεταφέρουν εμπιστευτικές πληροφορίες προς τρίτα μη εξουσιοδοτημένα πρόσωπα.

Πολιτική 8. Επιλογή Νέων Συστημάτων

α/α	Εφαρμογή
1	Οι προδιαγραφές για την προμήθεια νέων ή για την επέκταση υπαρχόντων συστημάτων, περιλαμβάνουν και απαιτήσεις ασφαλείας ανάλογα με την αποστολή την οποία επιτελούν η πρόκειται να επιτελέσουν.

Πολιτική 9. Ορθή Χρήση Εξοπλισμού

α/α	Εφαρμογή
1	Όλοι οι εργαζόμενοι της εταιρείας φροντίζουν ώστε να χρησιμοποιούν τον εξοπλισμό που τους παραχωρείται με υπευθυνότητα διαφυλάσσοντας, με αυτόν τον τρόπο, την εικόνα της εταιρείας, την ακεραιότητα του εξοπλισμού, καθώς και τις πληροφορίες που διαχειρίζονται. Δεν επιτρέπεται σε καμία περίπτωση η χρήση λογισμικού χωρίς άδεια, ή χρήση εξοπλισμού/λογισμικού για παράνομες ενέργειες.

Πολιτική 10. Mobile Computing

α/α	Εφαρμογή
1	Κατά κανόνα δεν χρησιμοποιούνται φορητοί υπολογιστές, εκτός από συγκεκριμένους χρήστες (διευθυντές) με χρήση ισχυρού κωδικού. Επίσης στα κινητά επιτρέπεται μόνο η σύνδεση του e-mail (Microsoft 365)

Πολιτική 11. Χρήση Αφαιρούμενων Μέσων

α/α	Εφαρμογή
1	Η αποθήκευση διαβαθμισμένων πληροφοριών σε κινητά μέσα (flash drives, φορητοί δίσκοι, μαγνητικά και οπτικά) αποθήκευσης πρέπει να αποφεύγεται. Σε περιπτώσεις που απαιτείται μεταφορά πληροφοριών μέσω κινητών μέσων πρέπει να δίνεται προσοχή ώστε να τηρούνται οι απαιτήσεις ασφάλειας.

Πολιτική 12. Ασφάλεια Πρόσβασης

α/α	Εφαρμογή
1	Η πρόσβαση στο εταιρικό δίκτυο καθώς στις συσκευές που είναι διασυνδεδεμένες προς αυτό είναι ελεγχόμενη. Αρμόδιοι για την σχεδίαση της πολιτικής πρόσβασης είναι ο Προϊστάμενος Τεχνικού μαζί με τον Διαχειριστή Συστημάτων (ΑΠΟΨΗ ΑΕ). Αρμόδιος για την υλοποίηση και περιοδικό έλεγχο της πολιτικής πρόσβασης είναι ο Διαχειριστής Συστημάτων (ΑΠΟΨΗ ΑΕ). Η πρόσβαση σε μεμονωμένα συστήματα που χρησιμοποιούνται στα πλαίσια της παροχής των υπηρεσιών είναι ελεγχόμενη (ARGUS ERP).

Πολιτική 13. Καθαρού Γραφείου (Clear Desk) και Καθαρής Οθόνης (Clear Screen)

α/α	Εφαρμογή
1	Για όλα τα μέλη του προσωπικού ακολουθείται η πολιτική καθαρού γραφείου (Clear Desk) και καθαρής οθόνης (Clear Screen).

Πολιτική 14. Κωδικοί πρόσβασης (Passwords)

α/α	Εφαρμογή
1	Οι κωδικοί πρόσβασης (passwords), όπου απαιτούνται να είναι ισχυρά. Κανόνες σχηματισμού ισχυρών passwords είναι ενδεικτικά : • Να αποτελούνται από τουλάχιστον οκτώ χαρακτήρες. • Να περιέχουν γράμματα (κεφαλαία και μικρά), αριθμούς και σύμβολα. • Να μην βρίσκονται σε λεξικό. • Να μην περιέχουν ημερομηνίες γενεθλίων, ονόματα συγγενικών

α/α	Εφαρμογή
	προσώπων κλπ. Κανόνες ορθής χρήσης κωδικών πρόσβασης (passwords) είναι ενδεικτικά οι ακόλουθοι : • Να μην τα αποκαλύπτετε σε κανένα, ούτε σε μέλη της οικογένειάς σας. • Να μην τα αποκαλύπτετε σε τηλεφωνικές συνδιαλέξεις, σε μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλα μέσα. • Δεν χρησιμοποιείται η επιλογή “Remember Password” στις εφαρμογές. Επιπλέον απαιτείται αλλαγή των κωδικών πρόσβασης κάθε τρείς μήνες και δεν επιτρέπεται η επαναχρησιμοποίηση των δύο τελευταίων κωδικών.

Πολιτική 15. Προστασία από Επιβλαβές Λογισμικό

α/α	Εφαρμογή
1	Ο διαχειριστής συστημάτων της ΑΠΟΨΗ ΑΕ ελέγχει καθημερινά τα αρχεία καταγραφής γεγονότων όλων των servers. Εφόσον διαγνώσει ένα σημαντικό γεγονός, θα φροντίζει γιά την ενημέρωση του συντονιστή της E.DIS.I.NET ΑΕ και θα σχεδιάζει σε συνεργασία μαζί του τις απαραίτητες διορθωτικές ενέργειες.
2	Απαγορεύεται αυστηρά η χρήση λογισμικού χωρίς άδεια χρήσης.
3	Απαγορεύεται αυστηρά η χρήση εξοπλισμού και λογισμικού για παράνομες ενέργειες.

Πολιτική 16. Επιχειρησιακή Συνέχεια (Business Continuity -BCP)

α/α	Εφαρμογή
1	Ο σκοπός ενός σχεδίου επιχειρησιακής συνέχειας είναι η επαναλειτουργία των κρίσιμων επιχειρησιακών διεργασιών μετά από μία απρογραμμάτιστη και απροσδόκητη διακοπή. Η ανάπτυξη ενός σχεδίου επιχειρησιακής συνέχειας θα πρέπει να λαμβάνει υπόψη τα ακόλουθα. 1. Καθορισμό των λειτουργικών απαιτήσεων κάθε κρίσιμης διεργασίας, των απαιτούμενων ελάχιστων πόρων για την επαναλειτουργία της, της διαθεσιμότητας τηλεπικοινωνιών και κρίσιμων δεδομένων. 2. Μία αποτίμηση και ιεράρχηση των κινδύνων. 3. Την επιλογή ενός οικονομικά βιώσιμου σεναρίου, την υλοποίηση και την συντήρησή του. 4. Την ανάπτυξη και συντήρηση ενός προγράμματος ενημέρωσης και επιμόρφωσης των αποδεκτών του σχεδίου καθώς και των μελών των ομάδων που θα το υποστηρίξουν.

α/α	Εφαρμογή
	Οι επιχειρηματικές διεργασίας που θα ενταχθούν στο σχέδιο πρέπει να είναι εγκεκριμένες από την Διοίκηση. Ο αποδεκτός μέγιστος χρόνος αποκατάστασης της λειτουργίας μίας κρίσιμης διεργασίας μετά από διακοπή πρέπει να είναι εγκεκριμένος από την Διοίκηση.

Πολιτική 17. Τηλεεργασία

α/α	Εφαρμογή
1	Ο εργαζόμενος έχει δύο επιλογές: - Είτε χρησιμοποιεί το εταιρικό laptop που του έχει διατεθεί - Είτε μπαίνει με AnyDesk στο PC του στην εταιρεία Απαγορεύεται η πρόσβαση στο δίκτυο της εταιρείας ή σε πόρους πελάτη από άλλο μηχάνημα
2	Στην περίπτωση που ο χρήστης έχει laptop θα πρέπει να κρυπτογραφεί είτε τον σκληρό είτε ευαίσθητα directories με έγγραφα ή κώδικα της εταιρείας. Ο σκοπός των παρακάτω είναι να μην διαρρεύσουν αρχεία προς τρίτους αν εσείς χάσετε την συσκευή σας (π.χ. κλοπή). Για τον σκοπό αυτό υποχρεούστε: - Αν έχετε Windows 10 Pro να ενεργοποιήσετε το Bitlocker - Στις υπόλοιπες περιπτώσεις να χρησιμοποιήστε το VeraCrypt (δωρεάν / open source) με το οποίο: o Φτιάχνετε έναν εικονικό δίσκο ορισμένης χωρητικότητας o Ρίχνετε μέσα τα αρχεία directories o Κρυπτογραφείτε το αρχείο του εικονικού δίσκου και κλειδώνετε με password που γνωρίζετε μόνο εσείς o Ενεργοποιείτε Mount του εικονικού δίσκου για χρήση
3	Οφείλουμε να είμαστε συνεχώς Online και διαθέσιμοι ως να είχαμε φυσική παρουσία ώστε να διευκολύνεται η ομαλή συνεργασία της ομάδας.