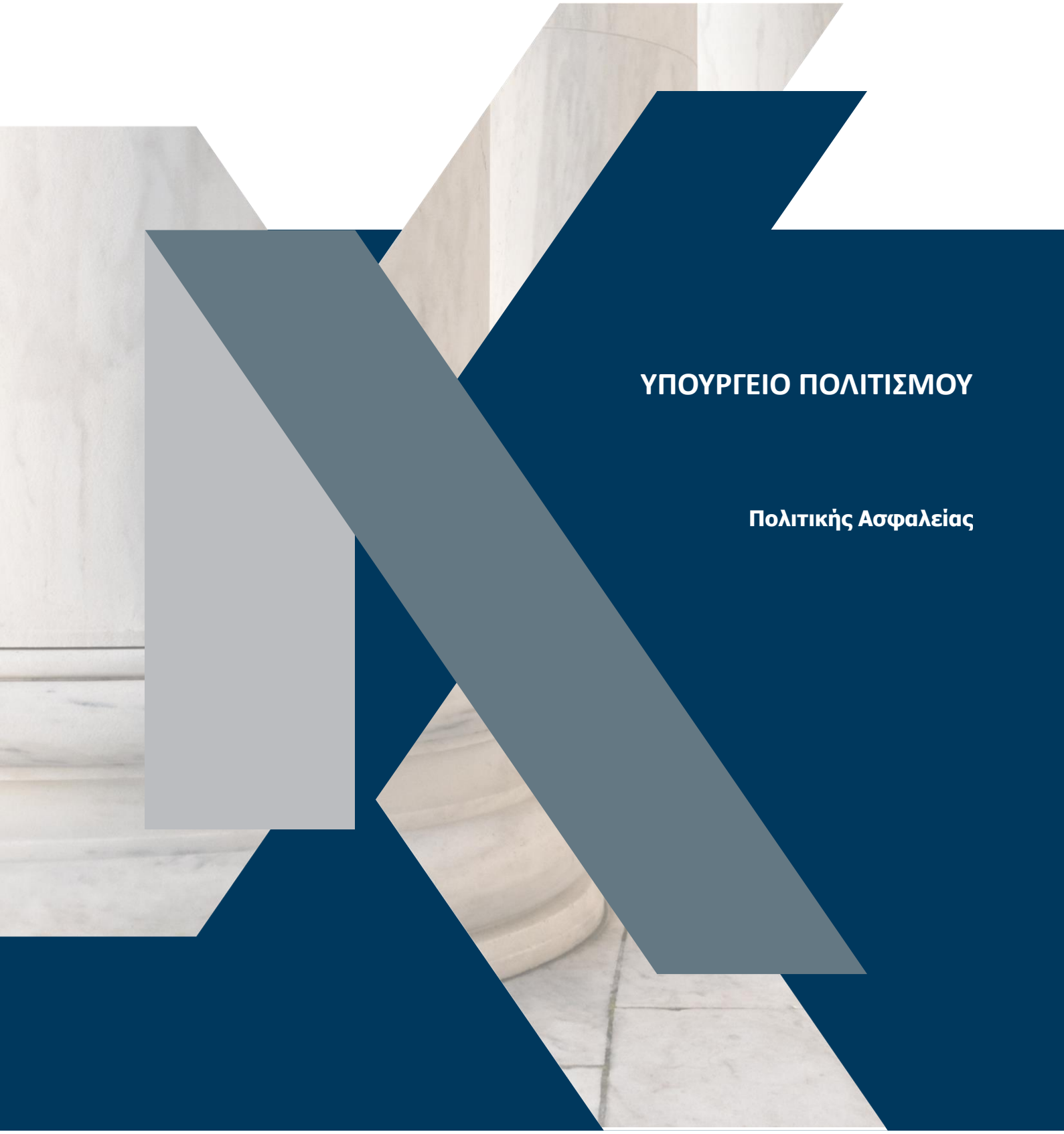

ΥΠΟΥΡΓΕΙΟ ΠΟΛΙΤΙΣΜΟΥ

Πολιτικής Ασφαλείας

Πίνακας περιεχομένων

Εισαγωγή

Οι πληροφοριακοί πόροι/συστήματα αποτελούν ιδιαίτερα κρίσιμα περιουσιακά στοιχεία του Υπουργείου Πολιτισμού και πρέπει να προστατεύονται ανάλογα με την αξία τους, με τρόπο ώστε να ενισχύεται η εμπιστοσύνη των πολιτών, να διασφαλίζεται η συμμόρφωση με το κανονιστικό πλαίσιο.

Το Υπουργείο Πολιτισμού αντιμετωπίζει σημαντικούς κινδύνους λόγω της αυξανόμενης εξάρτησης από τους πληροφοριακούς πόρους/συστήματα, των αυξανόμενων διασυνδέσεων των πληροφοριακών συστημάτων του με τρίτους (όπως παρόχους υπηρεσιών, προμηθευτές και συνεργάτες), των συνεχών οργανωτικών και τεχνολογικών αλλαγών που επιβάλλονται από τις ανάγκες των νέων καινοτόμων και υψηλής πολυπλοκότητας τεχνολογιών και επιχειρησιακών μοντέλων, αλλά και της καθημερινής εμφάνισης νέων απειλών που σχετίζονται με την τεχνολογία και τον κυβερνοχώρο. Το πλήθος των περιστατικών ασφάλειας, όπως για παράδειγμα είναι η διαρροή δεδομένων και κωδικών πρόσβασης εργαζομένων ή/και πολιτών, η παραβίαση ιστοσελίδων, η διάδοση κακόβουλου λογισμικού και οι επιθέσεις άρνησης υπηρεσίας (DDoS), έχει αυξηθεί σημαντικά, καθώς πολλές χώρες, κυβερνητικοί φορείς, οργανισμοί, χρηματοπιστωτικά ιδρύματα, επιχειρήσεις και ιδιώτες έχουν δεχθεί επιθέσεις που στοχεύουν στην υπονόμευση/καταστροφή της δημόσιας εικόνας τους και την απώλεια της φήμης ή/και στην επίτευξη οικονομικού οφέλους για τους κακόβουλους τρίτους.

Στο πλαίσιο αυτό, το Υπουργείο Πολιτισμού έχει υιοθετήσει μια στρατηγική διαφύλαξης της ασφάλειας των πληροφοριακών του πόρων και συστημάτων αναφορικά με την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητά τους, η οποία αποτυπώνεται στο παρόν έγγραφο.

Ορισμοί – Συντομογραφίες

0.1 Ορισμοί

ΟΡΟΣ	ΠΕΡΙΓΡΑΦΗ
Ασφάλεια Πληροφοριών	Υποδηλώνει το σύνολο των διοικητικών, τεχνικών και φυσικών μέτρων (πρακτικές και μέθοδοι), των οποίων η υλοποίηση και εφαρμογή διασφαλίζει την προστασία των πληροφοριακών πόρων/συστημάτων του Υπουργείου Πολιτισμού, συμπεριλαμβανομένων και των ενεργειών που προστατεύουν και προλαμβάνουν διαδικτυακές επιθέσεις σε ψηφιακούς χώρους (κυβερνοασφάλεια). Συγκεκριμένα, διασφαλίζει τις ιδιότητες εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα που χαρακτηρίζουν κάθε είδους πληροφοριακό πόρο/σύστημα. ***Εμπιστευτικότητα***: Η ιδιότητα που εξασφαλίζει ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να έχουν πρόσβαση σε συγκεκριμένους πληροφοριακούς πόρους/συστήματα. ***Ακεραιότητα***: Η ιδιότητα που εξασφαλίζει την προστασία των πληροφοριακών πόρων/συστημάτων από μη εξουσιοδοτημένη ή εξ αμελείας τροποποίηση.

	Διαθεσιμότητα: η Ιδιότητα που εξασφαλίζει τη διαθεσιμότητα των πληροφοριακών πόρων/συστημάτων σε εξουσιοδοτημένες οντότητες.
Πληροφοριακό Σύστημα	Πόροι και Συστήματα ΤΠΕ. Οι πόροι υλισμικού και λογισμικού και τα συστήματα ΤΠΕ, ως μέρος ενός μηχανισμού ή ενός δικτύου διασύνδεσης το οποίο υποστηρίζει τις λειτουργίες του Υπουργείου Πολιτισμού (π.χ. διακομιστές, εφαρμογές, λειτουργικά συστήματα, δίκτυα, κλπ.).
Εξωτερικοί Συνεργάτες/ΤρίταΜέρη	Πάροχοι υπηρεσιών, εταιρείες ενσωμάτωσης λύσεων πληροφορικής (integrators), προμηθευτές, τηλεπικοινωνιακοί πάροχοι, εταιρείες που παρέχουν υποστήριξη υποδομής δρώντας ως εξωτερικοί συνεργάτες του Υπουργείου Πολιτισμού
Κυβερνοχώρος	Ορίζεται το σύνθετο περιβάλλον που προκύπτει από τη μη φυσικής μορφής αλληλεπίδραση μεταξύ ανθρώπων, λογισμικού, πληροφοριών και υπηρεσιών στο διαδίκτυο, μέσω τεχνολογικών συσκευών και δικτύων που είναι συνδεδεμένα σε αυτό.
Πληροφοριακοί Πόροι	Συλλογή πληροφοριών, είτε υλικών είτε άυλων, που αξίζει να προστατεύονται (πληροφορίες αποθηκευμένες ψηφιακά σε πόρους/Συστήματα ΤΠΕ, φυσικό αρχείο κλπ.).
Αρχή της μηδενικής εμπιστοσύνης (zero trust principle)	Η αρχή της μηδενικής εμπιστοσύνης επιτάσσει ότι κανένας χρήστης, σύστημα, συσκευή και εφαρμογή, ακόμα και αν ανήκουν στο δίκτυο του Οργανισμού, δεν θεωρούνται από προεπιλογή έμπιστα εκτός και αν αυθεντικοποιηθούν. Η αρχή της μηδενικής εμπιστοσύνης αποτελεί ένα μοντέλο ασφάλειας, ένα σύνολο αρχών σχεδιασμού συστημάτων και μία συντονισμένη στρατηγική, που βασίζονται στην παραδοχή ότι οι απειλές ενυπάρχουν τόσο έξω όσο και μέσα από τις παραδοσιακές περιμέτρους των δικτύων. Ειδικότερα, οι θεμελιακές αρχές της Αρχής είναι: **"*never trust, always verify*"**: κάθε χρήστης, συσκευή, εφαρμογή και ροή δεδομένων θεωρούνται μη έμπιστα. Κάθε στοιχείο από τα παραπάνω πρέπει να αυθεντικοποιείται και κατόπιν να εξουσιοδοτείται ρητά με τα ελάχιστα απαιτούμενα προνόμια, **"*assume breach*"**: θεωρείται ότι οι συσκευές και το δίκτυο ενός Οργανισμού έχουν ενδεχομένως ήδη παραβιαστεί από κάποια κακόβουλη ομάδα. Εφαρμόζεται η αρχή **"*deny by default*"** (***άρνηση από προεπιλογή***) σε κάθε αίτημα πρόσβασης χρήστη, συσκευής, εφαρμογής και ροής δεδομένων. Η πρόσβαση δίδεται αφού εξεταστούν διεξοδικά πολλαπλές παράμετροι (π.χ. username χρήστη, όνομα και τοποθεσία συσκευής, ώρα, προηγούμενη καταγεγραμμένη συμπεριφορά του χρήστη κ.λπ.).
Ανάγκη Γνώσης (Need-to-know)	Η αρχή της ανάγκης γνώσης, σύμφωνα με την οποία παρέχεται πρόσβαση στον πληροφοριακό πόρο/σύστημα αποκλειστικά και μόνο στις οντότητες που είναι απαραίτητο να γνωρίζουν για να επιτελέσουν μια συγκεκριμένη διαδικασία/έργο.
Ανάγκη Χρήσης (Need-to-use)	Η αρχή της ανάγκης χρήσης, σύμφωνα με την οποία παρέχεται πρόσβαση στον πληροφοριακό πόρο/σύστημα αποκλειστικά και μόνο στις οντότητες που είναι

	απαραίτητο να την/τον χρησιμοποιήσουν για να επιτελέσουν μια συγκεκριμένη διαδικασία/έργο.
Ανάγκη Διατήρησης (Need-to-retain)	Η αρχή της ανάγκης διατήρησης, σύμφωνα με την οποία διατηρείται η πρόσβαση στον πληροφοριακό πόρο/σύστημα αποκλειστικά και μόνο για το χρονικό διάστημα που κρίνεται απαραίτητο, ώστε οι οντότητες να επιτελέσουν μια συγκεκριμένη διαδικασία/έργο.
Πλαίσιο Ασφάλειας Πληροφοριών	Η Στρατηγική, οι Πολιτικές, Διαδικασίες, Μεθοδολογίες, τα Τεχνολογικά Πρότυπα και οι Οδηγίες, τα οποία αποτελούν το σύνολο των διαδικαστικών, τεχνικών και φυσικών μέτρων (πρακτικές και μέθοδοι), των οποίων η υλοποίηση και εφαρμογή διασφαλίζει σε υψηλό βαθμό την προστασία των πληροφοριακών πόρων και των πληροφοριακών συστημάτων του Υπουργείου Πολιτισμού και συμβάλλουν στην επίτευξη των στόχων του.
Άμυνα εις βάθος	Η εις βάθος άμυνα αναφέρεται σε μια προσέγγιση ασφάλειας πληροφοριών στην οποία μια σειρά μηχανισμών και μέτρων ασφάλειας εφαρμόζονται σε επίπεδα για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών πόρων/συστημάτων.
Κακόβουλο λογισμικό (malware)	Λογισμικό σχεδιασμένο να προκαλέσει ζημιά ή να διακόψει τη λειτουργία του συστήματος/δικτύου στο οποίο εισέρχεται, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση και να συλλέξει ευαίσθητες πληροφορίες. Παραδείγματα κακόβουλου λογισμικού είναι οι ιοί, δούρειοι ίπποι, spyware κ.λπ.
Αρχή Ελάχιστων Δικαιωμάτων	Η αρχή των ελάχιστων προνομίων, σύμφωνα με την οποία μία οντότητα λαμβάνει τα λιγότερα δυνατά δικαιώματα πρόσβασης στους πληροφοριακούς πόρους/συστήματα, τα οποία κρίνονται απαιτητά για να επιτελέσει μια συγκεκριμένη διαδικασία/έργο.
Δοκιμές Παρείσδυσης (penetration testing)	Ένα σύνολο τεχνικών δοκιμών το οποίο επιχειρεί να ελέγξει την ασφάλεια συγκεκριμένων πληροφοριακών συστημάτων. Οι εν λόγω δοκιμές αποτελούν «εικονικές» επιθέσεις κατά των υπό εξέταση συστημάτων και αποσκοπούν στην εξεύρεση και εκμετάλλευση αδυναμιών ασφάλειας. Οι δοκιμές πρέπει να είναι εγκεκριμένες και να διεξάγονται από εξουσιοδοτημένους υπαλλήλους ή εξωτερικούς συνεργάτες.
Αξιολογήσεις Ασφάλειας Πληροφοριών (Security Assessments)	Οι αξιολογήσεις ασφάλειας πληροφοριών είναι περιοδικές ασκήσεις που δοκιμάζουν την ετοιμότητα ασφάλειας ενός οργανισμού. Περιλαμβάνουν ελέγχους για ευπάθειες στα συστήματα πληροφορικής, απ' όπου προκύπτουν συστάσεις για τη μείωση του κινδύνου μελλοντικών επιθέσεων. Οι αξιολογήσεις ασφάλειας πληροφοριών είναι επίσης χρήσιμες για την ενημέρωση των πολιτικών και διαδικασιών ενός οργανισμού.
Έλεγχος Ευπαθειών (Vulnerability Assessment)	Η αξιολόγηση και διαχείριση ευπαθειών και ενημερώσεων ασφάλειας περιλαμβάνει τον προσδιορισμό και την ιεράρχηση των τρωτών σημείων σε συστήματα υπολογιστών, εφαρμογών και δικτυακών υποδομών ώστε να αξιολογηθούν οι απειλές και οι κίνδυνοι που ενδέχεται να προκύψουν. Με την κατανόηση των τρωτών σημείων, το Υπουργείο Πολιτισμού μπορεί να διατυπώσει λύσεις και

	διορθώσεις για τα σημεία αυτά και να τα ενσωματώσει στο σύστημα διαχείρισης κινδύνων.
Κρυπτογράφηση	Η μαθηματική διαδικασία κωδικοποίησης πληροφοριών (π.χ. μηνυμάτων) σε συνθηματική μορφή με χρήση κάποιου κρυπτογραφικού κλειδιού, η οποία δύσκολα αναγνωρίζεται από ένα μη εξουσιοδοτημένο άτομο και θεωρητικά μπορεί να αναστραφεί μόνον από τον κάτοχο του κλειδιού.

0.2 Συντομογραφίες

ΟΡΟΣ	ΠΕΡΙΓΡΑΦΗ
ΥΑΠ	Υπεύθυνος Ασφάλειας Πληροφοριών
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
RfI	Request for Information/Interest
RfP	Request for Proposal
DC	Data Center: Κέντρο Δεδομένων
DRC	Data Recovery Center: Εναλλακτικό Κέντρο Δεδομένων

1. Σκοπός και Εύρος

1.1 Αντικείμενο της Πολιτικής

Η παρούσα πολιτική αποσκοπεί:

- Στην ενημέρωση του Προσωπικού του Υπουργείου Πολιτισμού για θέματα ασφάλειας πληροφοριών και στην εμπέδωση της ευθύνης που φέρει, για τη διαφύλαξη των στόχων αυτής.
- Στην αποτελεσματική και αποδοτική οργάνωση των μέτρων ελέγχου ασφάλειας πληροφοριών μέσω της κατάρτισης και εφαρμογής ενός πλαισίου κανόνων και διαδικασιών.
- Στη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών που παράγονται, διακινούνται, αποθηκεύονται και υφίστανται επεξεργασία από το Υπουργείο Πολιτισμού
- Στην αναγνώριση και αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών.
- Στη συμμόρφωση με το νομικό, θεσμικό και κανονιστικό πλαίσιο, στο οποίο υπάγεται το Υπουργείο Πολιτισμού, καθώς επίσης και στην συμμόρφωση με τα διεθνή πρότυπα και τις βέλτιστες πρακτικές.
- Στη δέσμευση της Διοίκησης για την επίτευξη και την διατήρηση ενός υψηλού επιπέδου ασφάλειας πληροφοριών, στην διάθεση στον ΥΑΠ όλων των απαραίτητων υλικοτεχνικών, οικονομικών και ανθρωπίνων πόρων για την άσκηση των καθηκόντων του καθώς και την εξασφάλιση στον ΥΑΠ των απαραίτητων πόρων για τη διατήρηση της εμπειρογνωσίας του καθώς και την προστασία του συνόλου των πληροφοριακών πόρων/συστημάτων.

1.2 Εύρος

Η παρούσα πολιτική καλύπτει το σύνολο των πληροφοριακών πόρων/συστημάτων του Υπουργείου Πολιτισμού και η πιστή εφαρμογή της αποτελεί ευθύνη τόσο του προσωπικού, όσο και των εξωτερικών συνεργατών/τρίτων μερών.

1.3 Αποδέκτες

Αποδέκτες της παρούσας πολιτικής είναι όλοι οι υπάλληλοι και οι εξωτερικοί συνεργάτες/τρίτα μέρη του Υπουργείου Πολιτισμού.

1.4 Διακυβέρνηση

Η παρούσα πολιτική αναθεωρείται κατ' ελάχιστον σε ετήσια βάση, εκτός αν προκύπτουν αλλαγές στο ισχύον ρυθμιστικό και κανονιστικό πλαίσιο που απαιτούν άμεση συμμόρφωση του Υπουργείου Πολιτισμού.

Υπεύθυνος αναθεώρησης είναι ο ΥΑΠ, ενώ εγκρίνεται από τον Υπηρεσιακό Γραμματέα του Υπουργείου Πολιτισμού.

1.5 Εμπλεκόμενα Μέρη

Η Διοίκηση του Υπουργείου Πολιτισμού
Οι επιμέρους Διευθύνσεις και Τμήματα του Υπουργείου Πολιτισμού
Το προσωπικό του Υπουργείου Πολιτισμού στο σύνολό του
Εξωτερικοί συνεργάτες του Υπουργείου Πολιτισμού (ανάδοχοι, προμηθευτές, συνεργαζόμενα τρίτα μέρη με τον Οργανισμό κ.ο.κ.)

2.0 Γενική Πολιτική Ασφάλειας Πληροφοριών

2.1 Οργανωτική δομή ασφάλειας πληροφοριών

Η ασφάλεια των πληροφοριών είναι κοινός στόχος για ολόκληρο το Υπουργείο Πολιτισμού. Προκειμένου να επιτευχθεί το απαιτούμενο επίπεδο ασφάλειας, είναι αναγκαία η στενή συνεργασία και ο συντονισμός όλων των Διευθύνσεων ανάλογα με τον βαθμό εμπλοκής τους. Για το λόγο αυτό, τα καθήκοντα ασφάλειας (ρόλοι και αρμοδιότητες) όπως και η διεκπεραίωση κρίσιμων διαδικασιών είναι σαφώς καθορισμένες σε όλο το εύρος του Υπουργείου Πολιτισμού, με στόχο την επίτευξη ομοιογένειας και συντονισμένων προσπαθειών κατά την επιλογή και εφαρμογή των απαραίτητων οργανωτικών, τεχνολογικών και φυσικών μέτρων ασφάλειας.

Η Διοίκηση του Υπουργείου Πολιτισμού έχει τη συνολική εποπτεία της λειτουργίας ασφάλειας πληροφοριών και καθορίζει τη στρατηγική κατεύθυνση και μεριμνά για τη συμμόρφωση του Οργανισμού με το Πλαίσιο Ασφάλειας Πληροφοριών, το κανονιστικό πλαίσιο και την προσαρμογή των σχετικών απαιτήσεων.

Όλες οι Διευθύνσεις του Υπουργείου Πολιτισμού συμβάλλουν στη διαμόρφωση ενιαίας κουλτούρας Ασφάλειας Πληροφοριών, συμμετέχουν έμπρακτα στην εφαρμογή του Πλαισίου Ασφάλειας Πληροφοριών και μεριμνούν για την προστασία των πληροφοριών που διαχειρίζονται.

Σε όλο το εύρος των δραστηριοτήτων του Υπουργείου Πολιτισμού εφαρμόζεται η αρχή του διαχωρισμού καθηκόντων, βάσει της οποίας οι αρμοδιότητες διαχωρίζονται σε τέτοια έκταση ώστε να περιορίζονται ή/και να εξαλείφονται οι πιθανότητες μη εξουσιοδοτημένης χρήσης ή κατάχρησης των αρμοδιοτήτων που ανατίθενται.

Ειδικότερα, καθορίζονται οι κάτωθι ρόλοι:

Υπεύθυνος Ασφάλειας Πληροφοριών: είναι ανεξάρτητο στέλεχος και εποπτεύεται απευθείας από την Ηγεσία του Υπουργείου Πολιτισμού. Τα κυριότερα καθήκοντά του περιλαμβάνουν τη μέριμνα για τη στρατηγική ασφάλειας πληροφοριών, την παροχή στρατηγικού επιπέδου Οδηγιών για θέματα κυβερνοασφάλειας, την επίβλεψη και παρακολούθηση του συστήματος διαχείρισης ασφάλειας πληροφοριών και την ευθύνη για την ανάπτυξη, διαμόρφωση, εφαρμογή, διαχείριση, συντήρηση και παρακολούθηση των πολιτικών, των βασικών αρχών, των διαδικασιών, των μηχανισμών και για την εν γένει ασφάλεια πληροφοριών σε ολόκληρο το Υπουργείο, σύμφωνα με τους στόχους του, τη στρατηγική πληροφορικής, τη διάθεση ανάληψης κινδύνου ασφάλειας πληροφοριών και το νομικό/κανονιστικό πλαίσιο.

Ιδιοκτήτης πληροφοριακών πόρων: Ορίζεται η Διεύθυνση (Κεντρική Υπηρεσία) η οποία έχει την ευθύνη αξιοποίησης των δεδομένων που καταχωρίζονται σε ένα πληροφοριακό σύστημα από την ίδια ή από τρίτους, ή/και είναι άρρηκτα συνδεδεμένα με το αντικείμενο και τις αρμοδιότητές της. Σημειώνεται ότι ως «Ιδιοκτήτης πληροφοριακών πόρων» δύναται να ορίζεται άνω της μίας Διεύθυνσης, καθώς ένα πληροφοριακό σύστημα μπορεί να εξυπηρετεί ανάγκες περισσότερων Διευθύνσεων (2.4).

Ιδιοκτήτης πληροφοριακών συστημάτων: Ορίζεται η Διεύθυνση Επικοινωνίας και Ανάπτυξης του Υπουργείου Πολιτισμού, η οποία έχει την ευθύνη διαχείρισης των πληροφορικών συστημάτων.

2.2 Συμμόρφωση με το νομικό/κανονιστικό πλαίσιο

Οι απαιτήσεις ασφάλειας πληροφοριών καθορίζονται σε μεγάλο βαθμό βάσει των νομικών/κανονιστικών και συμβατικών υποχρεώσεων. Τυχόν μη τήρησή τους ενδέχεται να επιφέρει σοβαρούς κινδύνους, όπως επιβολή προστίμων ή/και προσβολή της φήμης του Οργανισμού κλπ.

Οι απαιτήσεις ασφάλειας πληροφοριών που απορρέουν από τις νομοθετικές/κανονιστικές, συμβατικές ο διατάξεις με τις οποίες υποχρεούται να συμμορφώνεται το Υπουργείο Πολιτισμού, εντοπίζονται και παρακολουθούνται μέσω της τήρησης επικαιροποιημένου Μητρώου.

Λαμβάνονται τα κατάλληλα μέτρα προστασίας των πληροφοριακών πόρων/συστημάτων που διαχειρίζεται το Υπουργείο Πολιτισμού έναντι απώλειας, καταστροφής, παραποίησης, μη εξουσιοδοτημένης πρόσβασης και αποκάλυψης, σύμφωνα με τις νομοθετικές/κανονιστικές και συμβατικές απαιτήσεις. Επιπρόσθετα, ο αποδεκτός τρόπος αποθήκευσης, διαχείρισης και απόσυρσης/καταστροφής, καθώς και ο χρόνος διατήρησης για κάθε κατηγορία δεδομένων ορίζονται σύμφωνα με τις αντίστοιχες πολιτικές, το επίπεδο διαβάθμισης και τους ισχύοντες κανονισμούς. Έμφαση δίδεται στη διασφάλιση της συμμόρφωσης με το νομοθετικό/κανονιστικό πλαίσιο που αφορά την ιδιωτικότητα και την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η χρήση οποιουδήποτε υλικού χωρίς την άδεια του κατόχου των πνευματικών δικαιωμάτων ενδέχεται να επιφέρει νομικές κυρώσεις σύμφωνα με την κείμενη νομοθεσία. Περιοδικά διενεργούνται έλεγχοι, προκειμένου να διασφαλισθεί ότι δεν χρησιμοποιούνται, μέσω του δικτύου του Οργανισμού, μη εξουσιοδοτημένα λογισμικά και δεν δημιουργούνται παράνομα αντίγραφα προϊόντων πνευματικής ιδιοκτησίας τρίτων μερών.

Η εγκυρότητα, αξιοπιστία και συμμόρφωση των χρησιμοποιούμενων μηχανισμών κρυπτογράφησης με το ισχύον νομικό/κανονιστικό πλαίσιο διασφαλίζεται μέσω της διενέργειας σχετικών ελέγχων. Σε περιπτώσεις διασυνοριακής επικοινωνίας, λαμβάνονται υπόψη οι διάφοροι νόμοι και περιορισμοί κρυπτογράφησης που εφαρμόζονται στις χώρες αυτές.

Προκειμένου να διαπιστωθεί ότι η λειτουργία του Υπουργείου Πολιτισμού είναι σύμφωνη με το Πλαίσιο Ασφάλειας Πληροφοριών και ότι οι προβλεπόμενες πολιτικές και διαδικασίες καλύπτουν επαρκώς τις μεταβαλλόμενες απαιτήσεις ασφάλειας πληροφοριών, διενεργούνται ανεξάρτητες και τακτικές επιθεωρήσεις, στο πλαίσιο των οποίων αξιολογείται η αποδοτικότητα, η αποτελεσματικότητα και η καταλληλότητα των εφαρμοζόμενων μέτρων ασφάλειας.

2.3 Διαχείριση Επιχειρησιακής Συνέχειας του Οργανισμού

Ο περιορισμός των επιπτώσεων από πιθανή διακοπή των δραστηριοτήτων του Υπουργείου Πολιτισμού, αλλά και η διασφάλιση της συνέχειας των κρίσιμων λειτουργιών του σε περίπτωση μη διαθεσιμότητας, μπορούν να επιτευχθούν μόνον εφόσον υφίσταται αποτελεσματικός σχεδιασμός επιχειρησιακής συνέχειας, ο οποίος περιλαμβάνει τα ακόλουθα:

- **Πολιτική Επιχειρησιακής Συνέχειας**: Για τη μέγιστη δυνατή κάλυψη των απαιτήσεων ανάκαμψης των Διευθύνσεων και τυχόν κινδύνων/ευπαθειών ασφάλειας πληροφοριών.
- **Ανάλυση Λειτουργικών Επιπτώσεων**: Για την αναγνώριση και ανάλυση δραστηριοτήτων των

Διευθύνσεων, της κρισιμότητας αυτών, καθώς και την εκτίμηση των συνεπειών που μπορεί να έχει τυχόν διακοπή των δραστηριοτήτων της Διεύθυνσης και, κατ' επέκταση, του Υπουργείου Πολιτισμού. Επιπρόσθετα περιλαμβάνει αναλυτική καταγραφή των απαιτήσεων ανάκαμψης των Διευθύνσεων σε ανθρώπινο δυναμικό, εξοπλισμό και εφαρμογές.

- **Εκτίμηση Απειλών και Κινδύνων**: Για την εκτίμηση των απειλών και της πιθανότητας εκδήλωσης κινδύνων που μπορεί να έχουν επίπτωση στην ομαλή λειτουργία κρίσιμων δραστηριοτήτων και κατ' επέκταση στην Λειτουργική Συνέχεια.
- **Σχέδιο Επιχειρησιακής Συνέχειας**: Για τον καθορισμό του ανθρώπινου δυναμικού, των πληροφοριακών πόρων/συστημάτων, καθώς και των ενεργειών που απαιτούνται για την ανάκαμψη των δραστηριοτήτων κάθε Διεύθυνσης, σε περίπτωση διακοπής.
- **Σχέδιο Ανάκαμψης Συστημάτων από Καταστροφή**: Για την έγκαιρη ανάκαμψη μετά από καταστροφή όλων των πληροφοριακών πόρων/συστημάτων που υποστηρίζουν κρίσιμες δραστηριότητες.
- **Σχέδιο Εκτάκτου Ανάγκης και Εκκένωσης Κτηρίων**: Για την προετοιμασία και την ανάπτυξη διαδικασιών που θα βοηθήσουν το Υπουργείο Πολιτισμού να διαχειριστεί έκτακτα γεγονότα που πλήττουν τις κτηριακές εγκαταστάσεις και προκαλούν διακοπή των εργασιών, όπως π.χ. πυρκαγιά, σεισμός, απειλή για βόμβα.
- **Σχέδιο Διαχείρισης Κρίσεων**: Για τη διαχείριση σε επικοινωνιακό επίπεδο των κρίσεων ή έκτακτων καταστάσεων που ενδέχεται να προκύψουν και οι οποίες θα μπορούσαν να επηρεάσουν τη δραστηριότητα ή/και την εικόνα του Υπουργείου Πολιτισμού.

Το σύνολο των Σχεδίων δοκιμάζεται περιοδικά με στόχο την εξοικείωση των υπαλλήλων με τις διαδικασίες και τους χώρους ανάκαμψης και την επιβεβαίωση της πλήρους λειτουργίας των υποδομών. Τα σχέδια συντηρούνται ετησίως ή/και επικαιροποιούνται όποτε απαιτείται λόγω έκτακτων γεγονότων ή εργασιών που επηρεάζουν το Σχέδιο Επιχειρησιακής Συνέχειας, όπως π.χ. οργανωτικές αλλαγές, νέες κανονιστικές απαιτήσεις, νέες εργασίες .

Σε περίπτωση που δραστηριότητες του Υπουργείου Πολιτισμού έχουν ανατεθεί σε τρίτους (π.χ. πάροχο κρίσιμων υπηρεσιών/Outsourcing), τότε αυτοί πρέπει να διαθέτουν Σχέδιο Επιχειρησιακής Συνέχειας για τη διασφάλιση της διαθεσιμότητα των παρεχόμενων υπηρεσιών.

2.4 Διαβάθμιση πληροφοριακών πόρων/συστημάτων

Η διαβάθμιση των πληροφοριακών πόρων/συστημάτων ως προς την κρισιμότητα και την εμπιστευτικότητά τους αποτελεί διαδικασία, η οποία συμβάλλει στην ορθή επιλογή μέτρων ασφάλειας και στον κατάλληλο χειρισμό τους, από τους υπαλλήλους και τους εξωτερικούς συνεργάτες/τρίτα μέρη.

Κάθε πληροφοριακό σύστημα διαβαθμίζεται κατάλληλα, μέσω της αξιολόγησης των πιθανών επιπτώσεων που θα προκύψουν σε περίπτωση απώλειας της εμπιστευτικότητας (π.χ. διαρροή πληροφοριών σε μη εξουσιοδοτημένα μέρη), ακεραιότητας (π.χ. ακούσια ή εκούσια μη εξουσιοδοτημένη τροποποίηση) και διαθεσιμότητας (π.χ. καταστροφή ή αδυναμία προσβάσεως) των πληροφοριακών πόρων που επεξεργάζεται. Η διαβάθμιση υλοποιείται με χρήση συγκεκριμένου σχήματος, το οποίο καθορίζει τα χρησιμοποιούμενα επίπεδα και τα σχετικά κριτήρια κατηγοριοποίησης.

Σαν αποτέλεσμα αποδίδεται σε πληροφοριακούς πόρους/συστήματα, συγκεκριμένος χαρακτηρισμός αφενός ως προς την εμπιστευτικότητα και αφετέρου ως προς την κρισιμότητά τους, βάσει του οποίου καθορίζονται οι απαιτήσεις σήμανσης. Εξάλλου, η διαβάθμιση ως προς την κρισιμότητα λαμβάνεται υπ'όψη κατά την αξιολόγηση των κινδύνων ασφάλειας πληροφοριών.

Η διαβάθμιση των πληροφοριακών πόρων/συστημάτων επιτρέπει την άμεση αναγνώριση και την κατάλληλη διαχείριση αυτών, από τους υπαλλήλους και τους εξωτερικούς συνεργάτες/τρίτα μέρη. Η διαβάθμιση εφαρμόζεται και διατηρείται καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριακών πόρων/συστημάτων, εκτός ελάχιστων εξαιρέσεων.

Οι πληροφοριακοί πόροι/συστήματα τηρούνται σε Μητρώο, στο οποίο καταγράφεται το επίπεδο διαβάθμισης και ο Ιδιοκτήτης τους. Περισσότερες πληροφορίες στην 'Governance 2 - Μητρώο και Διαβάθμιση Πληροφοριακών Συστημάτων' στο *Παράρτημα Ι*.

2.5 Διαχείριση κινδύνων ασφάλειας πληροφοριών

Η διαχείριση των κινδύνων είναι μία σημαντική διαδικασία για την αποτελεσματική αναγνώριση, μετριασμό ή/και εξάλειψη των απειλών και ευπαθειών ασφάλειας πληροφοριών και μειώνει την επίπτωση ή/και την πιθανότητα πραγματοποίησής τους στις λειτουργίες του Υπουργείου Πολιτισμού. Μέσω αυτής, επιδιώκεται η αναγνώριση, η ανάλυση και η εκτίμηση των κινδύνων, προκειμένου να ιεραρχηθούν και να ληφθούν τα κατάλληλα μέτρα πρόληψης, περιορισμού και αντιμετώπισης.

Οι αξιολογήσεις κινδύνων ασφάλειας πληροφοριών διεξάγονται με ευθύνη του ιδιοκτήτη του εκάστοτε πληροφοριακού πόρου/συστήματος καθ' όλη τη διάρκεια του κύκλου ζωής του. Απαραίτητη προϋπόθεση για τη διεξαγωγή τους αποτελεί η αναγνώριση των εμπλεκόμενων πληροφοριακών πόρων/συστημάτων και ο προσδιορισμός της κρισιμότητας αυτών, με κριτήρια την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα.

Οι αξιολογήσεις κινδύνων ασφάλειας πληροφοριών βασίζονται στην εφαρμογή έγκυρης και δομημένης μεθοδολογίας, η οποία είναι ευθυγραμμισμένη με την στρατηγική προσέγγιση του Υπουργείου Πολιτισμού για τη διαχείριση του λειτουργικού κινδύνου.

Η Διοίκηση καθορίζει το επίπεδο της διάθεσης ανάληψης κινδύνων (risk appetite), βάσει του είδους και του επιπέδου κινδύνων που Υπουργείο Πολιτισμού διατίθεται να αναλάβει, ώστε να επιτύχει τους στρατηγικούς στόχους. Σύμφωνα με το ανωτέρω, προκύπτει η ανάγκη αντιμετώπισης των εντοπισθέντων κινδύνων που υπερβαίνουν το αποδεκτό επίπεδο. Αποφασίζονται ως εκ τούτου οι ενέργειες που απαιτούνται για τον περιορισμό τους εντός των ορίων ανοχής. Οι ενέργειες αυτές αποτυπώνονται σε σχέδια αντιμετώπισης, τα οποία θέτουν συγκεκριμένα χρονοδιαγράμματα, κατανέμουν τις επιμέρους αρμοδιότητες σε στελέχη ή Διευθύνσεις και εγκρίνονται από το κατάλληλο διοικητικό όργανο (π.χ. Εκτελεστική Επιτροπή).

Η πρόοδος υλοποίησης των σχεδίων αντιμετώπισης σε σχέση με τις συμφωνημένες προθεσμίες παρακολουθείται συστηματικά και παρέχεται σχετική ενημέρωση στον ΥΑΠ. Σε τακτική βάση επανεξετάζεται η αποτελεσματικότητα των μέτρων ελέγχου, προκειμένου να διασφαλίζεται ότι οι υπολειπόμενοι κίνδυνοι παραμένουν εντός των αποδεκτών ορίων, που θέτει η Διοίκηση.

2.6 Έλεγχος προσβάσεων

Η λογική πρόσβαση στα πληροφοριακά συστήματα του Υπουργείου Πολιτισμού αποτελεί τον βασικότερο παράγοντα για τη διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας αυτών. Σε κάθε περίπτωση εφαρμόζονται οι αρχές της «ανάγκης γνώσης», «ανάγκης χρήσης» και «ανάγκης διατήρησης» (need to know, need to use, need to retain) και γενικότερα η αρχή της μηδενικής εμπιστοσύνης (zero trust principle), προκειμένου κάθε χρήστης να έχει πρόσβαση και δικαιώματα επεξεργασίας μόνον στους πληροφοριακούς πόρους/συστήματα που απαιτούνται για την εκτέλεση των καθηκόντων του.

Τα δικαιώματα λογικής πρόσβασης των υπαλλήλων και των εξωτερικών συνεργατών/τρίτων μερών καθορίζονται σύμφωνα με τις ανάγκες και τις απαιτήσεις ασφάλειας πληροφοριών του Υπουργείου Πολιτισμού.

Για κάθε υπάλληλο, εξωτερικό συνεργάτη/τρίτο μέρος, που απαιτείται να αποκτήσει πρόσβαση σε πληροφοριακούς πόρους/συστήματα του Υπουργείου Πολιτισμού, υποβάλλεται αιτιολογημένο αίτημα προς τον ιδιοκτήτη/Διεύθυνση Επικοινωνίας και Ανάπτυξης. Στον χρήστη αποδίδεται μοναδικό αναγνωριστικό (username) και συνθηματικό (password), το οποίο αλλάζει κατά την πρώτη σύνδεση και ακολουθεί τις βέλτιστες πρακτικές και τις απαιτήσεις του Πλαισίου Ασφάλειας Πληροφοριών.

Περιοδικά διενεργείται ανασκόπηση των ενεργών χρηστών κάθε πληροφοριακού συστήματος και εξετάζεται κατά πόσον οι ενεργοί χρήστες διατηρούν την ανάγκη πρόσβασης και κατά πόσον έχουν τα ελάχιστα απαιτούμενα δικαιώματα για την εκτέλεση των καθηκόντων τους. Μη απαραίτητοι ή αδρανείς χρήστες απενεργοποιούνται ή διαγράφονται.

Σε περίπτωση αλλαγής θέσης υπαλλήλου, εξωτερικού συνεργάτη/τρίτου μέρους πραγματοποιείται κατάλληλη προσαρμογή των δικαιωμάτων πρόσβασης. Ομοίως, σε περίπτωση διακοπής της συνεργασίας για οποιοδήποτε λόγο, υπαλλήλου, εξωτερικού συνεργάτη/τρίτου μέρους πραγματοποιείται άμεση απενεργοποίηση του συνόλου των προσβάσεών του.

Οι υπάλληλοι, εξωτερικοί συνεργάτες/τρίτα μέρη χρησιμοποιούν τις εκάστοτε ισχύουσες μεθόδους ταυτοποίησης, ορίζουν δύσκολα προβλέψιμα συνθηματικά, που δεν συμπίπτουν με εκείνα που χρησιμοποιούν στην ιδιωτική τους ζωή, διατηρούν την εμπιστευτικότητα αυτών και τα αλλάζουν περιοδικά σε συμμόρφωση με την ισχύουσα πολιτική του εκάστοτε πληροφοριακού συστήματος.

Η πρόσβαση στον πηγαίο κώδικα των εφαρμογών λογισμικού που χρησιμοποιούνται στο Υπουργείο Πολιτισμού περιορίζεται μόνον στους εξουσιοδοτημένους υπαλλήλους, εξωτερικούς συνεργάτες/τρίτα μέρη. Η πρόσβαση των υπαλλήλων, εξωτερικών συνεργατών/τρίτων μερών που είναι υπεύθυνοι για την ανάπτυξη και υποστήριξη εφαρμογών λογισμικού σε παραγωγικά συστήματα απαγορεύεται ή είναι αυστηρώς ελεγχόμενη.

Κατά την ανάθεση δικαιωμάτων προσβάσεων και ρόλων λαμβάνεται μέριμνα για την τήρηση της αρχής του διαχωρισμού καθηκόντων και της σύγκρουσης συμφερόντων.

2.7 Απόκτηση, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων

Η κάλυψη των απαιτήσεων ασφάλειας πληροφοριών στα πληροφοριακά συστήματα που υποστηρίζουν τις λειτουργίες του Υπουργείου Πολιτισμού, προϋποθέτει την αποτελεσματική ενσωμάτωσή τους σε όλο τον κύκλο ζωής αυτών (Σχεδιασμός, Ανάπτυξη ή Προμήθεια, Ένταξη σε Λειτουργία & Συντήρηση, ΤελικήΑπόσυρση/Καταστροφή).

Η ανάλυση των απαιτήσεων ασφάλειας πληροφοριών εντάσσεται στην κατάρτιση των λειτουργικών καιτεχνικών προδιαγραφών κάθε πληροφοριακού συστήματος, είτε πρόκειται για νέο, είτε για βελτίωση υφιστάμενου.

Η ανάπτυξη πληροφοριακών συστημάτων πραγματοποιείται σε συγκεκριμένο και κατάλληλο

περιβάλλον (development environment) και βασίζεται σε βέλτιστες πρακτικές ασφάλειας ανάπτυξης πηγαίου κώδικα. Το περιβάλλον παραγωγής (production environment) κάθε πληροφοριακού συστήματος είναι πάντοτε πλήρως διαχωρισμένο από τα περιβάλλοντα όπου πραγματοποιείται η ανάπτυξη και οι δοκιμές (UAT environment).

Σε περίπτωση έτοιμης λύσης (commercial off the shelf) ή ανάπτυξης πληροφοριακού συστήματος από εξωτερικό συνεργάτη/τρίτο μέρος, οι απαιτήσεις ασφάλειας εντάσσονται σε κείμενα προδιαγραφών (π.χ. RfI/RfP), λαμβάνονται υπ' όψη κατά τη διάρκεια της αξιολόγησης των λύσεων και ενσωματώνονταιστις σχετικές συμβάσεις. Το Υπουργείο μεριμνά για τον έλεγχο της εφαρμογής τους από τον εξωτερικό συνεργάτη/τρίτο μέρος καθώς και τυχόν υπεργολάβους του, για την κάλυψη ολόκληρης της εφοδιαστικής αλυσίδας.

Ο έλεγχος κάθε νέου πληροφοριακού συστήματος διασφαλίζει την κάλυψη των απαιτήσεων ασφάλειαςπληροφοριών σε όλα τα επίπεδα λειτουργικότητας και πραγματοποιείται με χρήση μη παραγωγικών δεδομένων ή κατ' εξαίρεση ανωνυμοποιημένων/ψευδωνυμοποιημένων παραγωγικών δεδομένων εφόσον η χρήση αυτών είναι απαραίτητη για τον έλεγχο.

Όταν το πληροφοριακό σύστημα τίθεται σε παραγωγική λειτουργία παρακολουθείται έως ότου διαπιστωθεί η σταθερότητα και η αξιοπιστία του. Οποιαδήποτε τροποποίηση του πληροφοριακού συστήματος, είτε αφορά τον πηγαίο κώδικα είτε τη διαμόρφωση υποστηρικτικών υποδομών, πραγματοποιείται σύμφωνα με τεκμηριωμένη διαδικασία, στο πλαίσιο της οποίας τηρείται Μητρώο αλλαγών. Περιοδικά πραγματοποιείται έλεγχος για την επιτυχή εγκατάσταση κρίσιμων ενημερώσεων ασφάλειας πληροφοριών.

Κατά τη λήξη του χρόνου ζωής του πληροφοριακού συστήματος πραγματοποιείται απενεργοποίηση καιαπόσυρσή του, μέσω τεκμηριωμένης διαδικασίας, η οποία διασφαλίζει την ασφαλή καταστροφή των πληροφοριακών πόρων.

2.8 Επικοινωνίες και δίκτυα

Η ομαλή λειτουργία των πληροφοριακών συστημάτων του Υπουργείου Πολιτισμού και η ανταλλαγή πληροφοριακών πόρων, τόσο μεταξύ των Διευθύνσεων όσο και με τις εποπτικές αρχές, τους εξωτερικούς συνεργάτες/τρίτα μέρη και τους πελάτες, βασίζεται στην ορθή λειτουργία των μηχανισμών επικοινωνιών και των δικτύων μεταφοράς δεδομένων και φωνής.

Σε ό,τι αφορά στις δικτυακές υποδομές του Υπουργείου Πολιτισμού, διατηρείται κατάλληλη, επαρκής, ενημερωμένη καιέγκυρη τεκμηρίωση. Όλες οι συσκευές ή μηχανισμοί, που συνδέονται στα δίκτυα του Υπουργείου Πολιτισμού, αναγνωρίζονται μοναδικά με ονομασία, η οποία διέπεται από συγκεκριμένους κανόνες.

Τα τηλεπικοινωνιακά δίκτυα του Υπουργείου Πολιτισμού σχεδιάζονται σύμφωνα με τις βέλτιστες πρακτικές ασφαλούς αρχιτεκτονικής και οργανώνονται σε διακριτά τμήματα με ασφαλείς περιμέτρους, προκειμένου να εφαρμόζονται τα κατάλληλα μέτρα προστασίας των πληροφοριών και υπηρεσιών.

Τα συστήματα ασφάλειας διαμορφώνονται κατάλληλα, ώστε να επιβάλλουν την αρχή «άρνηση από προεπιλογή», να φιλτράρουν συγκεκριμένους τύπους ή πηγές δικτυακής κίνησης και να σταματούν τα εισερχόμενα και εξερχόμενα δικτυακά πακέτα, σε περίπτωση υποψίας για κακόβουλη δραστηριότητα. Οι ρυθμίσεις του εξοπλισμού ασφάλειας επικοινωνιών τεκμηριώνονται και επανεξετάζονται σε τακτική βάση. Σε περιπτώσεις αλλαγών, ακολουθείται η ισχύουσα διαδικασία διαχείρισης αλλαγών και λαμβάνονται αντίγραφα ασφάλειας των αρχείων παραμετροποίησης.

Κατάλληλοι μηχανισμοί ελέγχου πρόσβασης στα τηλεπικοινωνιακά δίκτυα του Οργανισμού διασφαλίζουν ότι μόνον εξουσιοδοτημένες συσκευές/χρήστες αποκτούν δυνατότητα επικοινωνίας. Η αρχιτεκτονική ασφάλειας ακολουθεί την προσέγγιση της «άμυνας σε βάθος», μέσω κλιμάκωσης του επιπέδου πολυπλοκότητας και αυστηρότητας των ελέγχων. Κατά την αρχική εγκατάσταση των συσκευών που συνδέονται σε τηλεπικοινωνιακά δίκτυα του Οργανισμού, απομακρύνονται τα μη απαραίτητα εργαλεία, χαρακτηριστικά, υποσυστήματα και λειτουργίες, παραμένουν

ενεργοποιημένες οι ελάχιστες απαιτούμενες θύρες και εφαρμογές, τροποποιούνται προκαθορισμένες παράμετροι και ελέγχεται ότι δεν αποκαλύπτονται πληροφορίες που θα μπορούσαν να διευκολύνουν την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε υποδομές του Υπουργείου Πολιτισμού. Οι συσκευές εξετάζονται σε τακτική βάση για την επαλήθευση των ρυθμίσεων διαμόρφωσης και την αξιολόγηση των ενεργειών χρηστών και διαχειριστών, ενημερώνονται περιοδικά και διαμορφώνονται κατάλληλα, ώστε να αντιμετωπίζονται αποτελεσματικά τυχόν ευπάθειες.

Για κάθε εισερχόμενη και εξερχόμενη μεταφορά δεδομένων μεταξύ των εσωτερικών τηλεπικοινωνιακών δικτύων του Υπουργείου Πολιτισμού και του Διαδικτύου υλοποιούνται μηχανισμοί εξέτασης περιεχομένου (content filtering), οι οποίοι ανιχνεύουν και αποτρέπουν τη μόλυνση συστημάτων με κακόβουλο λογισμικό, τη μη εξουσιοδοτημένη μετάδοση ευαίσθητων πληροφοριών, τη διακίνηση περιεχομένου που υπόκειται σε πνευματικά δικαιώματα και την υπερφόρτωση δικτυακών υπηρεσιών.

Τα ασύρματα και εξωτερικά προσβάσιμα τηλεπικοινωνιακά δίκτυα, οι εικονικές υποδομές που υλοποιούνται μέσω τεχνολογίας virtualization ή παρέχονται υπό τη μορφή υπηρεσιών cloud, προστατεύονται μέσω κατάλληλων μηχανισμών έναντι των απειλών ασφάλειας πληροφοριών. Οι υποδομές και οι μηχανισμοί διαχείρισης των υπηρεσιών τηλεφωνίας και τηλεδιάσκεψης με χρήση φωνής ή/και εικόνας απομονώνονται, τουλάχιστον λογικά, από τη λοιπή πληροφοριακή υποδομή, με στόχο τη διαφύλαξη της εμπιστευτικότητας της πληροφορίας και την αποφυγή κακόβουλων ενεργειών.

2.9 Φυσική και περιβαλλοντική ασφάλεια

Η απρόσκοπτη εκτέλεση των λειτουργιών, η αδιάλειπτη διατήρηση της ασφάλειας πληροφοριών του Υπουργείου Πολιτισμού και η ασφάλεια του προσωπικού προϋποθέτουν την ύπαρξη επαρκών φυσικών και περιβαλλοντικών μέτρων ασφάλειας για την προστασία περιοχών στις οποίες υπάρχουν άνθρωποι και πληροφοριακοί πόροι/συστήματα.

Ο έλεγχος για τη φυσική ασφάλεια περιλαμβάνει:

- μηχανισμούς ελέγχου φυσικής πρόσβασης
- μέτρα ελέγχου της περιμέτρου των εγκαταστάσεων
- διαδικασία διαχείρισης κλειδιών

Ο έλεγχος για την περιβαλλοντική ασφάλεια περιλαμβάνει:

- μέτρα πυρασφάλειας
- μέτρα προστασίας από πλημμύρα ή διαρροή νερού
- τήρηση προδιαγραφών πυρασφάλειας, αντιπλημμυρικής, αντικεραυνικής και αντισεισμικής προστασίας
- διαδικασία ανάκαμψης από φυσικές/περιβαλλοντικές καταστροφές.

Ιδιαίτερη προστασία λαμβάνεται για την ασφάλεια των πληροφοριακών συστημάτων, που φιλοξενούνται στο Κέντρο Δεδομένων της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης. Ο εξοπλισμός υποστηρίζεται από διατάξεις αδιάλειπτης παροχής ηλεκτρικής ενέργειας. Οι καλωδιώσεις υψηλών και ασθενών ρευμάτων προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και φθορά, ενώ οι υποστηρικτικές υποδομές τηλεπικοινωνιών διαθέτουν εγγυημένα επίπεδα ποιότητας και υποστήριξης (SLA) και διατάξεις εφεδρείας.

2.10 Προστασία πληροφοριακών πόρων/συστημάτων

Το Υπουργείο Πολιτισμού διασφαλίζει την ορθή και ασφαλή λειτουργία των πληροφοριακών του συστημάτων, επιδιώκοντας την αποτροπή πολλαπλών και ευρέως διαδεδομένων απειλών ασφάλειας

πληροφοριών.

Οι απειλές μόλυνσης από κακόβουλο λογισμικό προέρχονται ιδιαίτερα από ιστοσελίδες, μέσα κοινωνικής δικτύωσης, φορητά μέσα αποθήκευσης, ηλεκτρονικό ταχυδρομείο και λογισμικό ή αρχεία που μεταφέρονται μέσω του τηλεπικοινωνιακού δικτύου του Οργανισμού. Τα πληροφοριακά συστήματα είναι εφοδιασμένα με εγκεκριμένο και ενημερωμένο λογισμικό προστασίας από κακόβουλο λογισμικό. Το Υπουργείο Πολιτισμού παρακολουθεί και διαχειρίζεται μέσω κεντρικού μηχανισμού την υποδομή προστασίας των πληροφοριακών συστημάτων από κακόβουλο λογισμικό. Εξαιρέσεις, είτε ορισμένων συστημάτων από την απαίτηση εγκατάστασης προγράμματος προστασίας από κακόβουλο λογισμικό, είτε συγκεκριμένων αρχείων ή εφαρμογών από τη σάρωση μέσω του λογισμικού προστασίας, αξιολογούνται από τον ΥΑΠ και συνοδεύονται από επαρκή τεχνική τεκμηρίωση.

Τα πληροφοριακά συστήματα, οι εφαρμογές και οι δικτυακές υποδομές του Υπουργείου Πολιτισμού δύναται να παράγουν αναφορές σε σχέση με δραστηριότητες χρηστών, εξαιρέσεις, σφάλματα και γενικότερα συμβάντα ασφάλειας πληροφοριών. Τα εσωτερικά ρολόγια όλων των συστημάτων επεξεργασίας πληροφοριών του Υπουργείου Πολιτισμού είναι συγχρονισμένα με αξιόπιστη χρονική πηγή αναφοράς.

Οι παράμετροι επίδοσης και επάρκειας των εφαρμογών, συστημάτων και δικτύων του Υπουργείου Πολιτισμού παρακολουθούνται, προκειμένου να εντοπίζονται συμβάντα υποβάθμισης ή μη διαθεσιμότητας υπηρεσιών. Σε αυτό το πλαίσιο, προσδιορίζονται τα ασφαλή όρια χρήσης για τις υποδομές τεχνολογιών πληροφορικής και επικοινωνιών του Υπουργείου Πολιτισμού, τόσο κατά την κανονική λειτουργία τους όσο και σε περιόδους αιχμής, λαμβάνοντας υπ’ όψη τη διαβάθμισή τους.

Αντίγραφα ασφάλειας λαμβάνονται για το σύνολο των παραγωγικών πληροφοριακών συστημάτων που φιλοξενούνται στο κέντρο δεδομένων, σύμφωνα με τεκμηριωμένο πρόγραμμα, το οποίο καθορίζει τη συχνότητα λήψης και τον χώρο/χρόνο τήρησης αυτών, λαμβάνοντας υπ’ όψη το στόχο επαναφοράς (Recovery Point Objective-RPO) και τη διαβάθμιση των πληροφοριών και τις ανάγκες. Επιπρόσθετα, λαμβάνονται αντίγραφα των αρχείων διαμόρφωσης των δικτυακών συσκευών και των συστημάτων τηλεπικοινωνιών και ασφάλειας.

Η εγκατάσταση και αναβάθμιση λογισμικού στον εξοπλισμό πληροφορικής του Υπουργείου Πολιτισμού επιτρέπεται μόνον σε εξουσιοδοτημένα στελέχη της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης σύμφωνα με την αρχή των «ελαχίστων δικαιωμάτων».

Οι διαδικασίες διαχείρισης και λειτουργίας των πληροφοριακών συστημάτων που φιλοξενούνται στο κέντρου Δεδομένων του Υπουργείου Πολιτισμού είναι τεκμηριωμένες και διαθέσιμες στο αρμόδιο προσωπικό της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης.

Τα πληροφοριακά συστήματα του Υπουργείου Πολιτισμού ελέγχονται για την ύπαρξη τεχνικών αδυναμιών που θέτουν σε κίνδυνο την ασφάλεια πληροφοριών, τόσο πριν την ένταξη σε παραγωγική λειτουργία όσο και μετά, όπως απαιτείται κατά περίπτωση βάσει της κρισιμότητας και των χαρακτηριστικών τους. Οι έλεγχοι αδυναμιών ασφάλειας διενεργούνται με μέριμνα του ΥΑΠ σε συνεργασία με τη Διεύθυνση Ηλεκτρονικής Διακυβέρνησης και περιλαμβάνουν τεχνικές, όπως έλεγχο ευπαθειών (vulnerability assessment), δοκιμή διείσδυσης (penetration testing) και αξιολόγηση διαμόρφωσης (security configuration assessment).

Οι πληροφοριακοί πόροι/συστήματα του Υπουργείου Πολιτισμού αποτελούν αντικείμενο ελέγχου, τόσο από τη Διεύθυνση Εσωτερικού Ελέγχου όσο και από εξωτερικούς Φορείς (π.χ. εποπτικές αρχές, ανεξάρτητοι ελεγκτές), προκειμένου να διαπιστωθεί η συμμόρφωσή τους με τις απαιτήσεις του Πλαισίου Ασφάλειας Πληροφοριών, του νομικού/κανονιστικού πλαισίου και των διαδικασιών του Υπουργείου Πολιτισμού.

Η ανταλλαγή πληροφοριών μεταξύ του Υπουργείου Πολιτισμού και εξωτερικών συνεργατών/τρίτων μερών διασφαλίζεται μέσα από καθορισμένες διαδικασίες και μηχανισμούς ελέγχου, σε όλο το εύρος των χρησιμοποιούμενων μέσων επικοινωνίας. Σε κάθε περίπτωση και πριν την απόκτηση

οποιασδήποτε πρόσβασης σε δεδομένα, υπογράφεται Σύμβαση Εμπιστευτικότητας με το τρίτο μέρος.

2.11 Φορητές συσκευές και τηλεργασία

Οι φορητές συσκευές του Υπουργείου Πολιτισμού, καθώς και οι πληροφορίες που αφορούν το Υπουργείο Πολιτισμού και αποθηκεύονται σε αυτές, παραμένουν στην κυριότητα του Υπουργείου Πολιτισμού και παραχωρούνται σε υπαλλήλους για την εκπλήρωση των επαγγελματικών υποχρεώσεών τους. Οι υπάλληλοι διαχειρίζονται τις φορητές συσκευές που τους έχουνπαρασχεθεί σε συμμόρφωση με το Πλαίσιο Ασφάλειας Πληροφοριών. Το Υπουργείο Πολιτισμού διατηρεί το δικαίωμα να διαγράφει τα δεδομένα και να επιθεωρεί τις παρεχόμενες φορητές συσκευές, εάν υπάρχει υποψία για περιστατικά ασφάλειας πληροφοριών ή κακόβουλες ενέργειες. Το Υπουργείο Πολιτισμού επιτρέπει, όπου απαιτείται, να συνδεθούν σε πληροφοριακά συστήματα του, προσωπικές φορητές συσκευές (ιδιοκτησίας υπαλλήλων), οι οποίες υπόκεινται στις απαιτήσεις του Πλαισίου Ασφάλειας Πληροφοριών,όπως ακριβώς ισχύει για τις εκχωρημένες από τον Οργανισμό, φορητές συσκευές. Οι πληροφορίες του Υπουργείου Πολιτισμού, όπου είναι εφικτό, διαχωρίζονται από τα προσωπικά δεδομένα των υπαλλήλων.

Οι υπάλληλοι λαμβάνουν τα απαραίτητα μέτρα προστασίας των φορητών συσκευών που διαχειρίζονται, εκτός και εντός των υποδομών του Υπουργείου Πολιτισμού, προκειμένου να διασφαλισθεί ότι δεν τίθενται σε κίνδυνο οι πληροφοριακοί πόροι/συστήματα του Υπουργείου Πολιτισμού. Οι προσωπικές φορητές συσκευές ή οι φορητές συσκευές που ανήκουν στο Υπουργείο Πολιτισμού, δεν συνδέονται σε έμπιστα/εσωτερικά τηλεπικοινωνιακά δίκτυα του Υπουργείου Πολιτισμού, αλλά σε απομονωμένα τηλεπικοινωνιακά δίκτυα (ενσύρματα ή ασύρματα) με κατάλληλες ρυθμίσεις ασφάλειας.

Στον βαθμό που είναι εφικτό, η διαμόρφωση των φορητών συσκευών που συνδέονται στις υποδομές του Υπουργείου Πολιτισμού στηρίζεται σε πρότυπες ρυθμίσεις και λαμβάνονται όλα τα πρόσφορα τεχνικά μέτρα ασφάλειας. Οι υπάλληλοι αναφέρουν άμεσα στον ΥΑΠ και στον Διοικητικό Προϊστάμενό τους οποιαδήποτε απώλεια, κλοπή ή ασυνήθιστη λειτουργία φορητής συσκευής, καθώς και την πιθανολογούμενη ή επιβεβαιωμένη μη εξουσιοδοτημένη αποκάλυψη πληροφοριών του Υπουργείου Πολιτισμού.

Οι προσωπικές φορητές συσκευές τρίτων μερών επιτρέπεται να συνδέονται σε ιδιαίτερα διαμορφωμένα και πλήρως απομονωμένα ασύρματα τηλεπικοινωνιακά δίκτυα επισκεπτών/πελατών, τα οποία ενδέχεται να είναι διαθέσιμα σε εγκαταστάσεις του Υπουργείου Πολιτισμού όπου κρίνεται ότι η σκοπιμότητα υπερτερεί των κινδύνων που εισάγει η χορήγηση πρόσβασης σε μη ελεγχόμενες φορητές συσκευές.

Το Υπουργείο Πολιτισμού επιτρέπει σε εξουσιοδοτημένους υπαλλήλους και εξωτερικούς συνεργάτες/τρίτα μέρη να αποκτούν απομακρυσμένη πρόσβαση σε πληροφοριακά συστήματα και υποδομές, προκειμένου να εκτελέσουν τα επαγγελματικά τους καθήκοντα σύμφωνα με όσα ορίζονται στην Πολιτική Προστασίας Δεδομένων Εξ Αποστάσεως Εργασίας. Σε αυτό το πλαίσιο, λαμβάνεται ιδιαίτερη μέριμνα για τη λήψη επιπρόσθετων μέτρων ελέγχου και προστασίας των πληροφοριών του Υπουργείου Πολιτισμού, ώστε να αντιμετωπίζονται οι κίνδυνοι ασφάλειας πληροφοριών που προέρχονται από τον συγκεκριμένο τρόπο εργασίας. Στην εξ αποστάσεως εργασία, τυγχάνει εφαρμογής η Πολιτική Προστασίας Δεδομένων Εξ Αποστάσεως Εργασίας.

2.12 Διαχείριση ανθρωπίνου δυναμικού

Η διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών και η ουσιαστική εφαρμογή του Πλαισίου Ασφάλειας Πληροφοριών εναπόκειται πρωτίστως στο ανθρώπινο δυναμικό του Υπουργείου Πολιτισμού.

Κατά τη διαδικασία πρόσληψης και ειδικότερα κατά την κατάρτιση του ατομικού φακέλου, διενεργούνται κατάλληλοι έλεγχοι ταυτοποίησης, των απαιτούμενων τυπικών προσόντων και των λοιπών απαιτούμενων για την πρόσληψη δικαιολογητικών που προσκομίζει ο υπό πρόσληψη υπάλληλος, σε συμφωνία με τους σχετικούς νόμους και τους κανονισμούς. Κάθε νέος υπάλληλος

υπογράφει συμβατικό έγγραφο, το οποίο περιλαμβάνει, μεταξύ άλλων, όρους τήρησης της εμπιστευτικότητας και δέσμευση στην εφαρμογή του Πλαισίου Ασφάλειας Πληροφοριών.

Οι υπάλληλοι λαμβάνουν εισαγωγική ενημέρωση και συνεχή επιμόρφωση σχετικά με το Πλαίσιο Ασφάλειας Πληροφοριών και τις υποχρεώσεις τους ως προς την προστασία των προσωπικών δεδομένωνκαι άλλων εμπιστευτικών πληροφοριών .

Σε περίπτωση που υπάλληλος δεν ενεργεί (παραβιάζει) σύμφωνα με το Πλαίσιο Ασφάλειας Πληροφοριών, το θέμα αντιμετωπίζεται ως περιστατικό ασφάλειας πληροφοριών προκειμένου να ληφθούν τα απαραίτητα μέτρα ανάκαμψης από το ενδεχόμενο κενό ασφάλειας που έχει προκληθεί.

Σε περιπτώσεις τοποθέτησης, μετάθεσης, αλλαγής θέσης εργασίας ή τερματισμού απασχόλησης λαμβάνεται μέριμνα για την προσαρμογή των φυσικών και λογικών προσβάσεων και την επιστροφή τωνεκχωρημένων πληροφοριακών πόρων/συστημάτων, εφόσον απαιτείται.

2.13 Αποδεκτή χρήση πληροφοριακών συστημάτων

Οι υπάλληλοι και οι εξωτερικοί συνεργάτες/τρίτα μέρη κατανοούν τις υποχρεώσεις τους κατά τη χρήση πληροφοριακών πόρων/συστημάτων του Υπουργείου Πολιτισμού, προκειμένου να συνεισφέρουν ουσιαστικά στη διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών. Οι πόροι του Υπουργείου Πολιτισμού χρησιμοποιούνται μόνον για λειτουργικούς σκοπούς με αποδοτικό, λελογισμένο και σύννομο τρόπο, ώστε να εξυπηρετούνται οι λειτουργικές ανάγκες του.

Κατά τη χρήση των πληροφοριακών συστημάτων, οι υπάλληλοι και εξωτερικοί συνεργάτες/τρίτα μέρη εφαρμόζουν τα μέτρα που απαιτούνται για τη διαφύλαξη των λογαριασμών πρόσβασης που τους έχει αποδοθεί και την προστασία των πληροφοριακών πόρων του Υπουργείου Πολιτισμού από τους κινδύνους που σχετίζονται με κακόβουλο λογισμικό. Με την ολοκλήρωση των δραστηριοτήτων ή τον τερματισμό της συνεργασίας τους με το Υπουργείο Πολιτισμού, οι χρήστες επιστρέφουν όλους τους πληροφοριακούς πόρους/συστήματα που τους έχουν παρασχεθεί.

Οι υπάλληλοι και εξωτερικοί συνεργάτες/τρίτα μέρη συμμορφώνονται με τις απαιτήσεις που σχετίζονταιμε την προστασία των προσωπικών δεδομένων, ακολουθώντας τις πολιτικές, διαδικασίες και οδηγίες του Υπεύθυνου Προστασίας Δεδομένων, κατά τη χρήση των υπηρεσιών πληροφορικής που τους παρέχει το Υπουργείο Πολιτισμού. Η πρόσβαση στο Διαδίκτυο καθώς και η χρήση του ηλεκτρονικού ταχυδρομείου και άλλων δικτυακών υπηρεσιών, όπως είναι οι εφαρμογές διάσκεψης, επιτρέπεται μόνον στους εξουσιοδοτημένους υπαλλήλους και εξωτερικούς συνεργάτες/τρίτα μέρη, στο πλαίσιο της εκπλήρωσης των καθηκόντων τους.

Λαμβάνεται μέριμνα από τους υπαλλήλους και τους εξωτερικούς συνεργάτες/τρίτα μέρη για τον περιορισμό της παραγωγής και χρήσης έντυπων μέσων αποθήκευσης στα ελάχιστα απαιτούμενα, για την εκτέλεση των καθηκόντων τους.

Οι υπάλληλοι και εξωτερικοί συνεργάτες/τρίτα μέρη αναφέρουν άμεσα στον αρμόδιο Διοικητικό Προϊστάμενό τους και τον ΥΑΠ, γεγονότα μη αποδεκτής χρήσης πληροφοριακών πόρων/συστημάτων, τυχόν ασυνήθιστη δραστηριότητα στα πληροφοριακά συστήματα ή οποιοδήποτε άλλο πιθανό ή επιβεβαιωμένο συμβάν ασφάλειας πληροφοριών υποπίπτει στην αντίληψή τους.

2.14 Μέσα κοινωνικής δικτύωσης

Το Υπουργείο Πολιτισμού παρέχει κατευθύνσεις στους υπαλλήλους αναφορικά με την αποδεκτή συμπεριφορά τους στα μέσα κοινωνικής δικτύωσης.

Οι επίσημοι λογαριασμοί του Υπουργείου Πολιτισμού σε μέσα κοινωνικής δικτύωσης, καθώς και τα πνευματικά δικαιώματαπου σχετίζονται με το αναρτημένο περιεχόμενό τους, ανήκουν στον ίδιο τον Οργανισμό και χρησιμοποιούνται αποκλειστικά για τους σκοπούς προώθησης των συμφερόντων του.

Προκειμένου να διασφαλίζεται ότι το περιεχόμενο που δημοσιοποιείται προωθεί την καλή φήμη του

Υπουργείου Πολιτισμού, οι λογαριασμοί του προστατεύονται από κακόβουλη και μη εξουσιοδοτημένη πρόσβαση και αλλοίωση δεδομένων.

Επιλέγονται μόνον εκείνα τα μέσα κοινωνικής δικτύωσης που πληρούν τις προδιαγραφές ασφάλειας πληροφοριών και προστασίας δεδομένων, και σε αυτά αναρτάται υλικό από τους εξουσιοδοτημένους υπαλλήλους που φέρουν την ευθύνη διαχείρισης της παρουσίας του Υπουργείου Πολιτισμού. Η διαδικτυακή παρουσία στα μέσα κοινωνικής δικτύωσης παρακολουθείται συστηματικά, ώστε να εντοπίζεται και να αντιμετωπίζεταιεγκαίρως δημοσιευμένο υλικό που θα μπορούσε να έχει αρνητικό αντίκτυπο στο Υπουργείο Πολιτισμού.

Οι υπάλληλοι οφείλουν να συμμορφώνονται με τις πολιτικές του Υπουργείου Πολιτισμού κατά τη χρήση των μέσων κοινωνικής δικτύωσης στην ιδιωτική τους ζωή, καθώς δύναται να θεωρηθεί ότι - έστω και ατύπως - εκπροσωπούν δημοσίως το Υπουργείο Πολιτισμού . Οφείλουν να διασφαλίζουν ότι οι ιδιωτικές δραστηριότητές τους στα μέσα κοινωνικής δικτύωσης δεν αντιτίθενται στις δεσμεύσεις που έχουν αναλάβει στο πλαίσιο της συνεργασίας τους με το Υπουργείο και διαχωρίζουν σαφώς την ιδιωτική παρουσία τους στα μέσα κοινωνικής δικτύωσης, από την επίσημη εκπροσώπηση του Οργανισμού.

2.15 Διαχείριση περιστατικών ασφάλειας πληροφοριών

Σε περίπτωση εντοπισμού ή υποψίας οιασδήποτε παραβίασης του Πλαισίου Ασφάλειας Πληροφοριών, απαιτούνται άμεσες και αποτελεσματικές ενέργειες προκειμένου να ελαχιστοποιηθεί τυχόν ζημία σε φυσικά πρόσωπα, στην λειτουργία, την φήμη του Οργανισμού, και να αποφευχθούν σημαντικές οικονομικές ή νομικές επιπτώσεις.

Οι υπάλληλοι και οι εξωτερικοί συνεργάτες/τρίτα μέρη αναφέρουν συμβάντα ή ευπάθειες ασφάλειας, καθώς και περιστατικά παραβίασης της ασφάλειας πληροφοριών, αμέσως μόλις το αντιληφθούν.

Το Υπουργείο Πολιτισμού ενεργεί για τη διερεύνηση και την αντιμετώπιση του περιστατικού ασφάλειας πληροφοριών, με στόχο την ταχεία εξάλειψη των επιπτώσεων αυτού και την πλήρη αποκατάσταση των λειτουργιών του.

Μετά την ανάκαμψη, αξιολογείται η πρωταρχική αιτία (root cause analysis) του περιστατικού, τεκμηριώνονται οι άμεσες ή έμμεσες επιπτώσεις αυτού, καθώς και οι ενέργειες αντιμετώπισης που πραγματοποιήθηκαν, επανεξετάζεται η επάρκεια και αποτελεσματικότητα των χειρισμών για τον περιορισμό και την εξάλειψη των επιπτώσεων του περιστατικού ασφάλειας πληροφοριών και την αποκατάσταση των πληροφοριακών πόρων/συστημάτων και, όπου απαιτείται, υλοποιούνται οι απαραίτητες διορθωτικές ενέργειες.

Μετά την ολοκλήρωση χειρισμού του περιστατικού, συντάσσεται αναφορά, η οποία περιλαμβάνει όλες τις πληροφορίες που συλλέχθηκαν και προωθείται στις αρμόδιες Διευθύνσεις του Υπουργείου Πολιτισμού και στη Διοίκηση, αναλόγως της κρισιμότητας και του είδους του περιστατικού.

Το Υπουργείο Πολιτισμού συλλέγει και διατηρεί επαρκείς και τεκμηριωμένες αποδείξεις στο πλαίσιο της διαχείρισης σοβαρών περιστατικών ασφάλειας πληροφοριών, προκειμένου να διευκολύνει την πιθανή διενέργεια δικαστικής έρευνας. Εφόσον απαιτείται, επικοινωνεί και να συνεργάζεται με τις σχετικές εποπτικές και αστυνομικές αρχές (π.χ. Δίωξη Ηλεκτρονικού Εγκλήματος).

2.16 Διαχείριση εξωτερικών συνεργατών/τρίτων μερών

Το Υπουργείο Πολιτισμού μεριμνά για τη διαχείριση των κινδύνων ασφάλειας πληροφοριών, στους οποίους εκτίθενται οι πληροφοριακοί πόροι/συστήματα στο πλαίσιο των σχέσεων της με εξωτερικούς συνεργάτες/τρίτα μέρη, αναγνωρίζοντας ότι οποιαδήποτε νομική ή συμβατική υποχρέωση προστασίας δεδομένων εξακολουθεί να τη βαραίνει.

Οι εξωτερικοί συνεργάτες/τρίτα μέρη, οι οποίοι διαθέτουν λογική ή φυσική πρόσβαση σε πληροφοριακούς πόρους/συστήματα του Υπουργείου Πολιτισμού, είναι ενήμεροι για τις απαιτήσεις που απορρέουν από τις συμβάσεις και το Πλαίσιο Ασφάλειας Πληροφοριών και εφαρμόζουν τις προβλεπόμενες πρακτικές ασφάλειας.

Οι υποχρεώσεις των εξωτερικών συνεργατών/τρίτων μερών που απορρέουν από το πλαίσιο ασφάλειαςπληροφοριών, καθώς και οι ρόλοι και αρμοδιότητες εξωτερικών συνεργατών/τρίτων μερών όσον αφορά τη διασφάλιση της συμμόρφωσης, διατυπώνονται με πληρότητα και σαφήνεια και τεκμηριώνονται στις σχετικές συμβάσεις συνεργασίας. Πριν την παραχώρηση πρόσβασης σε πληροφοριακούς πόρους/συστήματα του Υπουργείου Πολιτισμού, διασφαλίζεται ότι έχει υπογραφεί κατάλληλη Σύμβαση Εμπιστευτικότητας.

Το Υπουργείο Πολιτισμού μεριμνά για τη συνεργασία του με αξιόπιστους προμηθευτές/παρόχους υπηρεσιών. Κατά το στάδιο επιλογής εξωτερικών συνεργατών/τρίτων μερών καθορίζονται οι ελάχιστες απαιτήσεις ασφάλειας πληροφοριών και προσδιορίζονται επαρκή, κατάλληλα και τεκμηριωμένα κριτήρια αξιολόγησης της ικανότητας των υποψήφιων προμηθευτών/παρόχων υπηρεσιών να καλύψουν τις εν λόγω απαιτήσεις ασφάλειας πληροφοριών και τις υποχρεώσεις συμμόρφωσης.

Το Υπουργείο Πολιτισμού μεριμνά για τη διατήρηση του απαιτούμενου επιπέδου παροχής υπηρεσιών ασφάλειαςπληροφοριών, σε ευθυγράμμιση με τις συμφωνίες που έχουν συναφθεί. Εφαρμόζει μέτρα ελέγχου των ενεργειών προμηθευτών/παρόχων υπηρεσιών σε πληροφοριακούς πόρους/συστήματα και επικυρώνει τακτικά την ισχύ, εγκυρότητα, πληρότητα και αποτελεσματικότητα των συμβάσεων, καθώς και τη συμμόρφωση με τους συμφωνημένους όρους ασφάλειας πληροφοριών. Η επίδοση των εξωτερικών συνεργατών/τρίτων μερών αξιολογείται τακτικά βάσει κατάλληλων κριτηρίων, προκειμένου να διασφαλίζεται η ικανοποίηση των συμβατικών απαιτήσεων και η επαρκής ικανότητα συνεχούς και ασφαλούς παροχής υπηρεσιών.

Σε περιπτώσεις εξωτερικών συνεργατών/τρίτων μερών που δεν συμμορφώνονται με το Πλαίσιο Ασφάλειας Πληροφοριών ή άλλων απαιτήσεων (π.χ. αδυναμία παροχής του συμφωνημένου επιπέδου υπηρεσιών), το Υπουργείο Πολιτισμού προχωρεί σε ενέργειες που ενδέχεται να περιλαμβάνουν την επαναδιαπραγμάτευση ή ακόμα και τη λύση των σχετικών συμβολαίων.

Κατά τον τερματισμό συνεργασιών με εξωτερικούς συνεργάτες/τρίτα μέρη, το Υπουργείο Πολιτισμού ενημερώνει σχετικάμε τις συμβατικές υποχρεώσεις τους και επιβεβαιώνει ότι έχουν αναιρεθεί οι σχετικές φυσικές και λογικές προσβάσεις, καθώς και ότι έχουν επιστραφεί οι πληροφοριακοί πόροι/συστήματα, ιδιοκτησίας του Υπουργείου Πολιτισμού.

2.17 Κρυπτογράφηση

Η χρήση κρυπτογράφησης αποτελεί ισχυρό εργαλείο για τη διαφύλαξη όχι μόνον της εμπιστευτικότητας, αλλά και της ακεραιότητας και αυθεντικότητας των πληροφοριακών πόρων που παράγονται, αποθηκεύονται και διακινούνται μέσω των πληροφοριακών συστημάτων του Υπουργείο Πολιτισμού. Η επιλογή των μηχανισμών κρυπτογράφησης, των σχετικών αλγορίθμων και του τρόπου εφαρμογής τους στο πλαίσιο των λειτουργιών του το Υπουργείο Πολιτισμού, αποτελεί συνάρτηση της κρισιμότητας των δεδομένων που πρέπει να προστατευθούν, καθώς και των νομικών/κανονιστικών απαιτήσεων.

Η επιλογή μεθόδων κρυπτογράφησης εξαρτάται από το επίπεδο διαβάθμισης που έχει αποδοθεί στους πληροφοριακούς πόρους/συστήματα, καθώς και από τους στόχους που επιδιώκονται. Όσο πιο υψηλό είναι το επίπεδο κρισιμότητας, τόσο πιο πολύπλοκοι και ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που επιλέγονται. Τα κρυπτογραφικά εργαλεία βασίζονται πάντοτε σε διεθνώς αναγνωρισμένα πρότυπα και πληρούν τουλάχιστον το ελάχιστο επίπεδο αποδεκτής ισχύος που έχουν ορίσει οι διάφοροι φορείς.

Η αποτελεσματικότητα των κρυπτογραφικών εργαλείων είναι άρρηκτα συνδεδεμένη με την ασφαλή διαχείριση των κρυπτογραφικών κλειδιών που χρησιμοποιούνται κατά την εφαρμογή διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης δεδομένων. Η παραβίαση και διαρροή των κρυπτογραφικώνκλειδιών δύναται να έχει ανεπανόρθωτες συνέπειες για το Υπουργείο Πολιτισμού, καθώς αναιρεί τα οφέλη της κρυπτογράφησης και επιτρέπει σε μη εξουσιοδοτημένα μέρη να υποκλέψουν ή ακόμα και να παραποιήσουν τα δεδομένα του Υπουργείου Πολιτισμού.

Τα κρυπτογραφικά κλειδιά χαρακτηρίζονται σύμφωνα με το υψηλότερο επίπεδο διαβάθμισης καιπροστατεύονται με χρήση όλων των αναγκαίων εργαλείων ασφάλειας. Η διανομή των κλειδιών γίνεται μόνον μέσω ασφαλών μέσων αποθήκευσης ή καναλιών επικοινωνίας, διαφορετικών από εκείνα που καλούνται να κρυπτογραφήσουν. Η διαρροή, απώλεια ή καταστροφή κλειδιών κρυπτογράφησης οδηγεί στην άμεση ανάκλησή τους και αποτελεί περιστατικό ασφάλειας πληροφοριών.

2.18 Ευαισθητοποίηση προσωπικού, εξωτερικών συνεργατών/τρίτων μερών

Το Υπουργείο Πολιτισμού οφείλει να ενημερώνει τους υπαλλήλους ανάλογα με τη θέση και το ρόλο τους σχετικά με:

- Τις συνέπειες των ενεργειών που θεωρούνται μη αποδεκτές (π.χ. μη εξουσιοδοτημένη χρήσητων πληροφοριακών συστημάτων).
- Τους κινδύνους που προκύπτουν από κακόβουλο λογισμικό.
- Τους κινδύνους που απορρέουν από τη μη ασφαλή χρήση των αφαιρούμενων μέσων και φορητών προσωπικών και κινητών συσκευών που ανήκουν στο Υπουργείο Πολιτισμού
- Την προστασία και την ιδιωτικότητα των πληροφοριακών πόρων.
- Την ιδιωτικότητα των επικοινωνιών.
- Το σύνολο των μηχανισμών που εφαρμόζονται από το Υπουργείο Πολιτισμού για την προστασία των πληροφοριακών πόρων/συστημάτων τόσο σε φυσικό όσο και

σε λογικό επίπεδο. Σε κάθε περίπτωση οι υπάλληλοι θα πρέπει να γνωρίζουν τους σκοπούς συλλογής των πληροφοριακών πόρων και τους ενδεδειγμένους τρόπους επεξεργασίας τους.

- Τα βήματα που θα πρέπει να ακολουθήσουν σε περιπτώσεις συμβάντων ασφάλειας πληροφοριών ώστε να μην καταστραφούν αποδεικτικά στοιχεία από πληροφοριακά συστήματα (π.χ. σταθμούς εργασίας και φορητές συσκευές, διακομιστές, συσκευές δικτύωσηςκτλ.).
- Τις συνέπειες (σε νομικό/κανονιστικό επίπεδο ή/και σε επίπεδο ασφάλειας πληροφοριών) πουεπιφέρει η εγκατάσταση, η χρήση και η τροποποίηση ελεύθερου λογισμικού ή λογισμικού ανοιχτού κώδικα.

Ο ΥΑΠ καλλιεργεί και προωθεί την αναγκαιότητα της ασφάλειας πληροφοριών και την προσωπική ευθύνη αναφορικά με αυτή. Για το σκοπό αυτό και με ευθύνη του, διοργανώνονται περιοδικά ενημερωτικές ημερίδες και συναντήσεις και δημοσιεύεται ενημερωτικό υλικό σε ειδικά διαμορφωμένο εσωτερικό ιστοχώρο. Επίσης, χρησιμοποιείται οποιοδήποτε άλλο πρόσφορο μέτρο και μέσο ώστε οι υπάλληλοι να παραμένουν ενήμεροι για τις τρέχουσες απειλές, όπως για παράδειγμα αποστολή ειδικών εκδόσεων (newsletters), αλλά και να τους υπενθυμίζονται σε τακτά χρονικά διαστήματα οι αρχές, οι κανόνες και οι εν γένει υποχρεώσεις τους σχετικά με την ασφάλεια πληροφοριών.

Το Υπουργείο Πολιτισμού υιοθετεί μία σειρά από διαφορετικές τεχνικές για την ενημέρωση και την εκπαίδευση των υπαλλήλων του και των τρίτων μερών στον τομέα της ασφάλειας πληροφοριών ανάλογα με τους ρόλους τους, τις ευθύνες τους και τις απαιτήσεις του.

Η Διεύθυνση Ανθρώπινου Δυναμικού, υπό την καθοδήγηση του ΥΑΠ, διασφαλίζει ότι τόσο οι νεοπροσληφθέντες υπάλληλοι όσο και οι ερχόμενοι για πρακτική άσκηση ενημερώνονται αναφορικά με το ισχύον πλαίσιο ασφάλειας πληροφοριών και δεσμεύονται επίσημα ως προς την τήρηση του.

Το Υπουργείο Πολιτισμού διασφαλίζει ότι εξωτερικοί συνεργάτες/τρίτα μέρη που έχουν πρόσβαση σε πληροφοριακούς πόρους/συστήματα, ενημερώνονται κατάλληλα για το πλαίσιο ασφάλειας πληροφοριών και για την παρούσα πολιτική, καθώς και τις υποχρεώσεις τους που απορρέουν από αυτό.

2.19 Χρήση υπηρεσιών Cloud

Η ευρεία διάδοση των υπηρεσιών υπολογιστικού νέφους (Cloud) οφείλεται στην εύκολη και κατ' απαίτηση πρόσβαση σε πληροφοριακά συστήματα, για τα οποία απαιτείται ελάχιστη προσπάθεια διαχείρισης. Ταυτόχρονα όμως, η χρήση τους θέτει μία σειρά προκλήσεων που πρέπει να αντιμετωπίζονται προκειμένου να διασφαλίζεται η ασφάλεια πληροφοριών του Υπουργείου Πολιτισμού

Το Υπουργείο Πολιτισμού καταγράφει τις υπηρεσίες Cloud που χρησιμοποιεί, καθώς και τα είδη των πληροφοριακών πόρων που μεταφέρονται στις υποδομές παρόχων των εν λόγω υπηρεσιών. Αν απαιτείται, ενημερώνει τις αρμόδιες εποπτικές αρχές κατά την έναρξη χρήσης υπηρεσιών Cloud, καθώς και όποτε υπάρχει αλλαγή στον τρόπο χρήσης των υπηρεσιών ή των πληροφοριακών πόρων που μεταφέρονται και τηρούνται στις υποδομές αυτές.

Πριν τη χρήση υπηρεσιών Cloud αξιολογούνται οι κίνδυνοι που είναι δυνατόν να

οδηγήσουν σε διακοπή δραστηριοτήτων του Υπουργείου Πολιτισμού, διαρροή δεδομένων, παραβίαση του Πλαισίου Ασφάλειας Πληροφοριών ή/και του νομικού/κανονιστικού πλαισίου και προσδιορίζονται σαφώς τα απαραίτητα μέτρα ασφάλειας πληροφοριών προκειμένου να διασφαλίζονται οι διαχειριζόμενες πληροφορίες κατά τη δημιουργία, επεξεργασία, αποθήκευση, μεταφορά και καταστροφή τους.

Κατά τη σύναψη συμφωνιών με παρόχους υπηρεσιών Cloud, προσδιορίζονται οι υποχρεώσεις των τελευταίων όσον αφορά την υλοποίηση των μέτρων ασφάλειας που εμπίπτουν στο πεδίο ευθύνης τους,τους γεωγραφικούς περιορισμούς αναφορικά με τη διαβίωση δεδομένων του Υπουργείου Πολιτισμού, καθώς και ο τύποςκαι η συχνότητα αποστολής αναφορών προς το Υπουργείο Πολιτισμού, προκειμένου να παρακολουθείται η αποτελεσματικότητα των μέτρων αυτών. Στις συμβάσεις με τους παρόχους υπηρεσιών Cloud καθορίζεται το επίπεδο των παρεχόμενων υπηρεσιών και οι μέθοδοι παρακολούθησης αυτού, διευκρινίζεται αν ο πάροχος των υπηρεσιών χρησιμοποιεί υπεργολάβους και τεκμηριώνεται η απαίτησηδιενέργειας επιθεωρήσεων των εγκαταστάσεων και των υποδομών τους.

Κατά τον τερματισμό της συμβατικής σχέσης με παρόχους υπηρεσιών Cloud, το Υπουργείο Πολιτισμού λαμβάνει τα απαραίτητα μέτρα για την αποτελεσματική μεταφορά των υπηρεσιών σε άλλους παρόχους ή σε ιδιόκτητες υποδομές, προκειμένου να διασφαλίζεται η συνέχεια των λειτουργιών του.

ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΗΣ

Η Πολιτική αυτή θα πρέπει να αναθεωρείται για να αντικατοπτρίζει τυχόν αλλαγές ή τροποποιήσεις της σχετικής νομοθεσίας για την προστασία των προσωπικών δεδομένων.

Η Πολιτική αυτή εκπονήθηκε από την Διεύθυνση Ηλεκτρονικής Διακυβέρνησης σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων του Υπουργείου Πολιτισμού.

Τα παραρτήματα αποτελούν αναπόσπαστο μέρος της παρούσας πολιτικής.

Η Πολιτική αυτή εγκρίθηκε από το Υπουργείο Πολιτισμού την 27η Οκτωβρίου 2025.

3.0 Παραρτήματα – Θεματικές Πολιτικές Ασφαλείας

3.1 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.1.1 ΕΙΣΑΓΩΓΗ

Η ορθή διαχείριση των πληροφοριακών πόρων αποτελεί θεμελιώδη παράμετρο για την προστασία, τη διαθεσιμότητα και την ακεραιότητα των δεδομένων ενός οργανισμού. Η αποτελεσματική αναγνώριση, καταγραφή και ταξινόμηση των Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΠΕΣ) συμβάλλει στην εφαρμογή στοχευμένων μέτρων ασφάλειας, στη διασφάλιση της συμμόρφωσης με κανονιστικά πλαίσια και στη διαχείριση κινδύνων που σχετίζονται με τα συστήματα πληροφορικής.

Η παρούσα πολιτική καθορίζει το πλαίσιο για τη δημιουργία, διαχείριση και τακτική αναθεώρηση ενός ολοκληρωμένου Μητρώου Πληροφοριακών Συστημάτων, το οποίο περιλαμβάνει όλα τα κρίσιμα στοιχεία των συστημάτων του οργανισμού και καθορίζει τους υπεύθυνους διαχείρισης αυτών. Παράλληλα, θεσπίζει τις βασικές αρχές για τη διαβάθμιση των συστημάτων ανάλογα με την κρισιμότητά τους, ώστε να διασφαλίζεται η βέλτιστη κατανομή πόρων και προτεραιοτήτων ασφάλειας.

3.1.2 ΣΚΟΠΟΣ

Σκοπός της Πολιτικής είναι να:

- εξασφαλίσει ότι όλα τα πληροφοριακά συστήματα του οργανισμού καταγράφονται σε ένα επίσημο Μητρώο Πληροφοριακών Συστημάτων,
- καθορίσει ρόλους και υπευθυνότητες για τη διαχείριση, προστασία και ενημέρωση των πληροφοριακών πόρων,
- εισαγάγει ενιαία κριτήρια για τη διαβάθμιση των συστημάτων βάσει της επιχειρησιακής τους σημασίας και των επιπτώσεων που θα είχε τυχόν απώλειά τους.

3.1.3 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική αφορά όλα τα ΠΕΣ, όλων των Υπηρεσιών του Υπουργείου.

3.1.4 ΜΗΤΡΩΟ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ο οργανισμός διατηρεί και ενημερώνει τακτικά ένα Μητρώο Πληροφοριακών Συστημάτων, το οποίο αποτελεί την επίσημη και μοναδική πηγή αναφοράς για όλα τα συστήματα πληροφορικής που χρησιμοποιούνται.

Το Μητρώο περιλαμβάνει, κατ’ ελάχιστο, τα ακόλουθα στοιχεία για κάθε σύστημα:

- Ονομασία.
- Λειτουργικός σκοπός και επιχειρησιακή χρήση.
- Τμήμα ή οργανωτική μονάδα που το διαχειρίζεται.
- Υπεύθυνος Πληροφοριακού Συστήματος (System Owner).
- Τεχνικός Υπεύθυνος (System Administrator).
- Τεχνολογική υποδομή (λογισμικό, εξοπλισμός, φυσική ή/και λογική τοπολογία).

- Επίπεδο πρόσβασης και ομάδες χρηστών.
- Ημερομηνία δημιουργίας και τελευταίας αναθεώρησης της καταχώρισης.
- Τρέχουσα κατάσταση (ενεργό, υπό ανάπτυξη, προς απόσυρση).

3.1.5 ΔΙΑΒΑΘΜΙΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Όλα τα πληροφοριακά συστήματα του οργανισμού πρέπει να κατηγοριοποιούνται ανάλογα με την κρισιμότητά τους για τη λειτουργία του οργανισμού και τις επιπτώσεις που θα είχε τυχόν απώλειά τους ή παραβίαση ασφάλειας. Η κατηγοριοποίηση καθορίζει τα μέτρα ασφάλειας, την προτεραιοποίηση των ενημερώσεων και τον τρόπο διαχείρισης κινδύνου.

Η αξιολόγηση γίνεται σε τρεις άξονες: **Εμπιστευτικότητα**, **Ακεραιότητα**, **Διαθεσιμότητα** και προκύπτει με τη συμπλήρωση ενός απλού ερωτηματολογίου (*βλέπε παρακάτω '3.1.7 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ'*) από τον Υπεύθυνο του Πληροφοριακού Συστήματος. Η συνολική κρισιμότητα κάθε συστήματος προκύπτει από τη βαθμολογία που συγκεντρώνει στους τρεις άξονες. Τα συστήματα υψηλής κρισιμότητας υπόκεινται σε αυξημένα μέτρα ασφάλειας, όπως συχνότερα αντίγραφα ασφαλείας, μηχανισμούς παρακολούθησης λειτουργίας και ειδικές διαδικασίες ανάκαμψης σε περίπτωση βλάβης ή παραβίασης.

3.1.5 ΕΠΙΚΑΙΡΟΠΟΙΗΣΗ

Το Μητρώο Πληροφοριακών Συστημάτων πρέπει να επανεξετάζεται τουλάχιστον ανά εξάμηνο, ώστε να διασφαλίζεται η εγκυρότητα των στοιχείων του και η ορθή αποτύπωση των υπευθύνων και της κατάστασης κάθε συστήματος. Η συνολική ευθύνη για τη διατήρηση και ενημέρωση του Μητρώου ανήκει στη ΔΗΔ.

Οι υπεύθυνοι των Πληροφοριακών Συστημάτων οφείλουν να διασφαλίζουν την ακρίβεια των καταχωρήσεων που αφορούν τα συστήματά τους και να ενημερώνουν άμεσα το Μητρώο, μέσω της ΔΗΔ, σε περίπτωση αλλαγών.

3.1.6 ΑΝΑΘΕΩΡΗΣΗ

Η παρούσα πολιτική υπόκειται σε τακτική αναθεώρηση τουλάχιστον μία φορά ετησίως ή νωρίτερα, σε περίπτωση σημαντικών οργανωτικών, τεχνολογικών ή κανονιστικών αλλαγών.

3.1.7 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η αξιολόγηση γίνεται σε τρεις άξονες: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα. Για κάθε άξονα παρέχεται ένα σύνολο ερωτήσεων οι οποίες βαθμολογούνται με τρεις πιθανές τιμές:

- 0 = Χαμηλή / Όχι
- 1 = Μέτρια / Μερικώς
- 2 = Υψηλή / Ναι

Α. Εμπιστευτικότητα (Confidentiality)

1. Περιέχει το σύστημα προσωπικά ή ευαίσθητα προσωπικά δεδομένα (GDPR);
2. Εμπεριέχει διαβαθμισμένες πληροφορίες ή πνευματική ιδιοκτησία;
3. Υπάρχουν νομικές/συμβατικές υποχρεώσεις για τη μη αποκάλυψη;
4. Διαρροή των δεδομένων θα προκαλούσε σοβαρή ζημία στη φήμη του Υπουργείου ή σε τρίτους;

Άθροισμα (0–8):

- 0–2 = Χαμηλή Εμπιστευτικότητα
- 3–5 = Μέτρια
- 6–8 = Υψηλή

Β. Ακεραιότητα (Integrity)

1. Αν αλλοιωθούν τα δεδομένα, θα προκληθεί οικονομική/νομική ζημία;
2. Το σύστημα επηρεάζει κρίσιμες αποφάσεις/αναφορές (π.χ. οικονομικά, ιατρικά, ρυθμιστικά δεδομένα);
3. Υπάρχουν απαιτήσεις για απόλυτη ακρίβεια/συμμόρφωση;
4. Η αλλοίωση δεδομένων μπορεί να βλάψει ανθρώπους, περιβάλλον ή την αξιοπιστία του Υπουργείου;

Άθροισμα (0–8):

- 0–2 = Χαμηλή Ακεραιότητα
- 3–5 = Μέτρια
- 6–8 = Υψηλή

Γ. Διαθεσιμότητα (Availability)

1. Πόσο γρήγορα πρέπει να αποκατασταθεί το σύστημα αν πέσει; (0 = >72h, 1 = 8–72h, 2 = <8h).
2. Ποιες είναι οι λειτουργικές επιπτώσεις από διακοπή λειτουργίας 1 ώρας ή 1 ημέρας (το χειρότερο σενάριο);
3. Επηρεάζει το σύστημα βασικές επιχειρησιακές λειτουργίες ή άλλα συστήματα;

4. Η μη διαθεσιμότητα μπορεί να προκαλέσει νομικές κυρώσεις ή απώλεια συμμόρφωσης;

5. Υπάρχει κίνδυνος για ανθρώπους/περιβάλλον από διακοπή λειτουργίας;

6. Υπάρχει εφεδρικό σύστημα λειτουργίας;

Άθροισμα (0–12):

- 0–3 = Χαμηλή Διαθεσιμότητα
- 4–6 = Μέτρια
- 7–9 = Υψηλή
- 10–12 = Κρίσιμη

3.1.8 ΠΡΟΦΙΛ ΣΥΣΤΗΜΑΤΟΣ

Μετά τη συμπλήρωση του ερωτηματολογίου, το άθροισμα των βαθμολογιών σε κάθε άξονα συνθέτει το προφίλ του συστήματος.

Ένα σύστημα θεωρείται Κρίσιμο όταν πληρείται μία από τις ακόλουθες προϋποθέσεις:

(i) έχει αξιολογηθεί ως Υψηλό ή Κρίσιμο σε οποιονδήποτε από τους τρεις άξονες (Εμπιστευτικότητα, Ακεραιότητα ή Διαθεσιμότητα), ή

(ii) το άθροισμα των τριών βαθμολογιών (Α + Β + Γ) υπερβαίνει το όριο των 18 βαθμών (δηλαδή ποσοστό άνω του 65% της μέγιστης βαθμολογίας).

3.2 ΠΟΛΙΤΙΚΗ ΓΙΑ ΤΡΙΤΟΥΣ / ΑΝΑΔΟΧΩΝ ΚΑΙ ΣΥΝΕΡΓΑΤΩΝ

3.2.1 ΕΙΣΑΓΩΓΗ

Αναγνωρίζοντας τον κίνδυνο που υπάρχει κατά τη διαχείριση πληροφοριών και συστημάτων πληροφορικής του Υπουργείου Πολιτισμού από τρίτους, το Υπουργείο Πολιτισμού εφαρμόζει την παρούσα Πολιτική με στόχο τον έλεγχο του κινδύνου αυτού και τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών του.

Η παρούσα Πολιτική θεσπίζει τις αρχές, τα κριτήρια και τις διαδικασίες συνεργασίας του Υπουργείου Πολιτισμού με τρίτους: αναδόχους και συνεργάτες (είτε πρόκειται για φυσικά, είτε για νομικά πρόσωπα) που έχουν πρόσβαση, διαχειρίζονται ή υποστηρίζουν πληροφοριακά συστήματα, δίκτυα και ψηφιακά περιουσιακά στοιχεία (assets) καθώς και με αναδόχους παροχής υπηρεσιών όπως οι τηλεπικοινωνιακές υπηρεσίες.

Η Πολιτική συντάσσεται βάσει των προτύπων ISO/IEC 27001:2022 και 27036-2, της Οδηγίας (ΕΕ) 2022/2555 (NIS2), του Κανονισμού (ΕΕΕ 2016/679 (GDPR), του Ν4624/2019 και της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

3.2.2 ΣΚΟΠΟΣ

Σκοπός της Πολιτικής είναι:

- Η διαφάνεια στις σχέσεις του Υπουργείου Πολιτισμού με τους αναδόχους έργων, προμηθευτές και συνεργάτες του, που έχουν πρόσβαση στις πληροφορίες και στα συστήματα πληροφορικής του Υπουργείου.
- Η δημιουργία ενός ασφαλούς, υγιούς και φιλικού περιβάλλοντος συνεργασίας με σεβασμό στα ανθρώπινα δικαιώματα και τις ανθρώπινες αξίες.
- Η δημιουργία σχέσεων αμοιβαίας εμπιστοσύνης και σεβασμού
- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από τις δραστηριότητες των αναδόχων και των συνεργατών του Υπουργείου Πολιτισμού.
- Η διασφάλιση της προστασίας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και συστημάτων του Υπουργείου Πολιτισμού, κατά την φυσική ή ηλεκτρονική πρόσβαση αυτών από τους αναδόχους/προμηθευτές/ συνεργάτες.

Η συμμόρφωση με την παρούσα Πολιτική αποτελεί υποχρέωση όλων των συνεργαζόμενων μερών και προϋπόθεση για τη σύναψη ή συνέχιση συνεργασίας με το Υπουργείο Πολιτισμού.

3.2.3 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η Πολιτική εφαρμόζεται σε:

- Αναδόχους έργων πληροφορικής
- Συνεργάτες που παρέχουν υπηρεσίες φιλοξενίας, συντήρησης ή ανάπτυξης συστημάτων
- Προμηθευτές λογισμικού ή εξοπλισμού
- Εξωτερικούς παρόχους υποστήριξης ή cloud υπηρεσιών

- Οποιονδήποτε συνεργάτη (είτε πρόκειται για φυσικό, είτε για νομικό πρόσωπο) που αποκτά πρόσβαση σε πληροφοριακά συστήματα ή δεδομένα του Υπουργείου.

Το Υπουργείο Πολιτισμού διατηρεί ενημερωμένο αρχείο αναδόχων έργων/προμηθευτών και συνεργατών που σχετίζονται με τη λειτουργία των πληροφοριακών συστημάτων, στο οποίο αναγράφονται:

- Στοιχεία Συνεργάτη/Προμηθευτή/Αναδόχου Έργου
- Στοιχεία επικοινωνίας υπεύθυνου ατόμου
- Υπηρεσίες που παρέχονται από τον εξωτερικό συνεργάτη
- Προσβάσεις στα συστήματα του Υπουργείου
- Είδος πληροφορίας που επεξεργάζονται, αποθηκεύουν ή διαβιβάζουν
- Διάρκεια πρόσβασης στα συστήματα του Υπουργείου

Το Υπουργείο Πολιτισμού επιδεικνύει τη δέουσα επιμέλεια κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές, λαμβανομένων υπόψη των κινδύνων τρίτων μερών, μεταξύ άλλων, της εξάρτησης από τον εκάστοτε προμηθευτή, της ομοιογένειας των συστημάτων, της διαχείρισης περιστατικών και της ευθύνης σε σχέση με την ασφάλεια δικτύων και πληροφοριών. Η αποδοχή της Πολιτικής από τους αναδόχους/συνεργάτες τεκμαίρεται με την υπογραφή της σχετικής σύμβασης ή συμφωνίας εμπιστευτικότητας (NDA).

3.2.4 ΓΕΝΙΚΕΣ ΑΡΧΕΣ

Όλα τα τρίτα μέρη οφείλουν να τηρούν/εφαρμόζουν:

- Πιστά τα προβλεπόμενα από τη μελέτη, τη διακήρυξη, την Τεχνική Συγγραφή Υποχρεώσεων και τη σύμβαση του έργου/προμήθειας ως επίσης και τις οδηγίες/εντολές των αρμοδίων υπηρεσιών του Υπουργείου Πολιτισμού.
- Ασφάλεια πληροφοριών σύμφωνα με διεθνή πρότυπα και κανονισμούς (ISO/IEC 27001, ISO/IEC 27036, NIS2).
- Ελαχιστοποίηση πρόσβασης: Δικαιώματα χρήσης περιορίζονται στο απολύτως αναγκαίο
- Εμπιστευτικότητα: Υπογραφή συμφωνιών NDA για την προστασία δεδομένων
- Συμμόρφωση με GDPR, εθνική νομοθεσία και πολιτικές ασφάλειας του Υπουργείου Πολιτισμού.
- Διαχείριση κινδύνου: Υποχρέωση άμεσης αναφοράς περιστατικών ασφαλείας.

3.2.5 ΟΔΗΓΙΕΣ ΚΑΙ ΚΑΝΟΝΕΣ ΑΣΦΑΛΕΙΑΣ

3.2.5.1 Αναγνώριση των Κινδύνων που Σχετίζονται με Εξωτερικούς Συνεργάτες

Πριν την έναρξη εργασιών ή σύναψη συμβάσεων, η Ομάδα Έργου του Υπουργείου Πολιτισμού προβαίνει σε αξιολόγηση κινδύνου εξωτερικού συνεργάτη για τον οποίο κρίνει ότι αυτό είναι απαραίτητο, λαμβάνοντας υπόψη την:

- Την κατηγοριοποίηση των πληροφοριών που θα λαμβάνει.

- Την φυσική ή/και ηλεκτρονική πρόσβαση του στα κτήρια/συστήματα του Υπουργείου.
- Τον τρόπο σύνδεσης δικτύων μεταξύ του Υπουργείου και του εξωτερικού συνεργάτη.
- Τις υφιστάμενες μεθόδους και μέτρα ασφάλειας που εφαρμόζει.
- Εάν η υφιστάμενη υποδομή του συνεργάτη είναι φυσική ή σε υπολογιστικό νέφος.
- Εάν ο συνεργάτης βρίσκεται σε χώρα που θεωρείται κρίσιμη για το Υπουργείο για την διασφάλιση των δεδομένων που θα λαμβάνει ο συνεργάτης.

Με αυτό τον τρόπο, αναγνωρίζονται πιθανά αναγκαία επιπρόσθετα μέτρα ασφαλείας που χρειάζονται να αναληφθούν από τον εξωτερικό συνεργάτη.

Η αξιολόγηση κινδύνου τρίτων διενεργείται σύμφωνα με το άρθρο 21 παρ. 2 της Οδηγίας (ΕΕ) 2022/2555 και καλύπτει την εφοδιαστική αλυσίδα (supply chain risk)

3.2.5.2 Γενικές Υποχρεώσεις Αναδόχων και Συνεργατών

Οι ανάδοχοι και συνεργάτες του Υπουργείου Πολιτισμού οφείλουν.

- Να γνωρίζουν και να εφαρμόζουν την Πολιτική Ασφάλειας του Υπουργείου. Για το προσωπικό των αναδόχων που εκτελούν εργασίες στις εγκαταστάσεις του Υπουργείου ισχύουν οι ίδιοι κανόνες με το προσωπικό του Υπουργείου.
- Να αναφέρουν κάθε περιστατικό που μπορεί να θέσει σε κίνδυνο τα πληροφοριακά συστήματα του Υπουργείου. Ειδικότερα, κάθε περιστατικό ασφάλειας πρέπει να γνωστοποιείται στο Τμήμα Υποδομών και Δικτύων εντός 24 ωρών από τη διαπίστωση και να συνοδεύεται από τεχνική αναφορά εντός 72 ωρών.
- Να διατηρούν την εμπιστευτικότητα των δεδομένων στα οποία αποκτούν πρόσβαση.
- Να μην αποκαλύπτουν πληροφορίες ή άλλα στοιχεία που συνδέονται με
- Το περιεχόμενο ή την ουσία των επικοινωνιών του Υπουργείου με Υπηρεσίες και πολίτες.
- Στοιχεία σχετικά με υπηρεσίες επικοινωνιών που παρέχονται ή πρόκειται να παρασχεθούν σε ένα πρόσωπο.
- Άλλα προσωπικά δεδομένα χρηστών των τηλεπικοινωνιακών υπηρεσιών, όπως αριθμούς τηλεφώνου ή διευθύνσεις.
- Να συντάσσουν δελτία παρεχόμενων υπηρεσιών κατά τα προβλεπόμενα στη σύμβαση έργου.
- Να συμμετέχουν σε τακτικές συναντήσεις για συζήτηση των συμφωνηθέντων, της απόδοσης και της εφαρμογής της σύμβασης, των πολιτικών και των διαδικασιών.

3.2.6 Προκηρύξεις Διαγωνισμών και Συμβάσεις

- Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των πληροφοριακών συστημάτων του Υπουργείου Πολιτισμού περιλαμβάνουν όρους που εξασφαλίζουν συμβατικά και τεχνικά την τήρηση της Πολιτικής Ασφάλειας του Υπουργείου. Στις

συβάσεις γίνεται ιδιαίτερη αναφορά στην τήρηση της Πολιτικών Απορρήτου και Προστασίας Προσωπικών Δεδομένων.

- Οι συμβάσεις έργων που σχετίζονται με τη λειτουργία των πληροφοριακών συστημάτων του Υπουργείου περιλαμβάνουν ρήτρες σε περίπτωση μη συμμόρφωσης με την Πολιτική Ασφάλειας.
- Η είσοδος σε χώρους πληροφοριακών συστημάτων, για την εξέταση επί τόπου του έργου πριν την κατάθεση προσφοράς, γίνεται μετά από έγκριση του αρμόδιου τμήματος και σύμφωνα με την πολιτική ασφαλείας του Υπουργείου.
- Για την πρόσβαση σε προσωπικά δεδομένα υπαλλήλων του Υπουργείου ή σε δεδομένα που αφορούν τις επικοινωνίες των υπαλλήλων του ΥΠΠΟ απαιτείται η λήψη άδειας από το Υπεύθυνο Τμήμα/Γραφείο.

3.2.7 Υπεύθυνος Παρακολούθησης Έργου

- Το Υπουργείο Πολιτισμού, με απόφαση του Προϊσταμένου της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης, ορίζει συγκεκριμένο φυσικό πρόσωπο, ως Υπεύθυνο Παρακολούθησης Έργου Πληροφοριακών Συστημάτων, που θα είναι υπεύθυνο για τη εποπτεία του εκάστοτε συνεργάτη/αναδόχου ως προς την τήρηση των συμβατικών υποχρεώσεων του.
- Οι όροι που αφορούν την τήρηση της Πολιτικής Ασφάλειας περιλαμβάνονται και στις προκηρύξεις των έργων.
- Για το προσωπικό των αναδόχων και συνεργατών που έχουν πρόσβαση στις εγκαταστάσεις και τον εξοπλισμό πληροφορικής του Υπουργείου απαιτείται ενυπόγραφη άδεια από τον Υπεύθυνο Παρακολούθησης Έργου.
- Ο ανάδοχος/προμηθευτής/συνεργάτης με την ανάθεση του έργου υποχρεούται να καταθέσει πίνακα σύμφωνα με το υπόδειγμα του Υπουργείου, στον Υπεύθυνο Παρακολούθησης Έργου, με το προσωπικό που θα χρησιμοποιήσει.
- Ο Υπεύθυνος Παρακολούθησης Έργου δίδει στο γραφείο υποδοχής/φύλακα πίνακα με το προσωπικό που έχει πρόσβαση στο Υπουργείο για το συγκεκριμένο έργο.
- Τα άτομα που πραγματοποιούν εργασίες στα πληροφορικά συστήματα του Υπουργείου καταγράφονται και η ταυτότητά τους ελέγχεται.
- Εξωτερικά συνεργεία συντήρησης, επισκευών και καθαρισμού των χώρων πληροφοριακών συστημάτων συνοδεύονται διαρκώς από αρμόδιους υπαλλήλους του Υπουργείου και οι εργασίες εκτελούνται μετά από σχετική έγκριση του αρμόδιου Τμήματος .
- Ο ανάδοχος έργου δεν μπορεί να εκχωρήσει δικαιώματα χρήσης του ευαίσθητου εξοπλισμού σε τρίτους χωρίς ενυπόγραφη άδεια του Υπουργείου.
- Το Υπουργείο και ο Υπεύθυνος Παρακολούθησης Έργου, έχουν το δικαίωμα παρακολούθησης και ελέγχου των εργασιών καθώς και της ανάκλησης εργασιών που δεν συμμορφώνονται με τις εκάστοτε πολιτικές ασφαλείας.

3.2.8 Ειδικές Υποχρεώσεις Αναδόχων και Συνεργατών

Οι ανάδοχοι και συνεργάτες που αποκτούν πρόσβαση σε συστήματα ή δίκτυα πρέπει:

- Να χρησιμοποιούν μοναδικά προσωπικά διαπιστευτήρια (όχι κοινόχρηστους λογαριασμούς)
- Να εφαρμόζουν ισχυρή αυθεντικοποίηση (π.χ. MFA)
- Να διασφαλίζουν την προστασία κωδικών και κλειδιών πρόσβασης
- Να χρησιμοποιούν ασφαλείς μεθόδους σύνδεσης (VPN, κρυπτογράφηση).
- Να αποφεύγουν την αποθήκευση δεδομένων σε μη εγκεκριμένες συσκευές.
- Να προστατεύουν τα δεδομένα προσωπικού χαρακτήρα και ευαίσθητες επιχειρησιακές πληροφορίες.
- Να αποθηκεύουν/επεξεργάζονται δεδομένα μόνο σε εγκεκριμένα περιβάλλοντα.
- Να εφαρμόζουν μηχανισμούς backup και disaster recovery.
- Να τηρούν κανόνες ταξινόμησης και χειρισμού δεδομένων (Confidential, Internal, Public).
- Να επιστρέφουν ή καταστρέφουν όλα τα δεδομένα και υλικά μετά τη λήξη της συνεργασίας.
- Να εφαρμόζουν νομοθετικές υποχρεώσεις π.χ. GDPR, πνευματική ιδιοκτησία, κανονισμούς της ΕΕ.
- Να λαμβάνουν μέτρα ασφαλείας για την προστασία περιουσιακών στοιχείων, για παράδειγμα: διαδικασίες σε σχέση με υλισμικά και λογισμικά, μέτρα για προστασία από κακόβουλα λογισμικά, περιορισμοί στην αντιγραφή ή αποκάλυψη πληροφοριών.

Ο ανάδοχος έργου δεν μπορεί να εκχωρήσει δικαιώματα χρήσης του ευαίσθητου εξοπλισμού σε τρίτους χωρίς ενυπόγραφη άδεια από το Υπουργείο Πολιτισμού.

Ο ανάδοχος έργου είναι υπεύθυνος για την επιβεβαίωση της ταυτότητας και της επαγγελματικής επάρκειας του προσωπικού του που θα εμπλακεί σε οποιαδήποτε εργασία του Υπουργείου και ως εκ τούτου θα έχει πρόσβαση σε κτήριο, συστήματα ή πληροφορίες του Υπουργείου.

Ο ανάδοχος έργου θα πρέπει να ενημερώνει τον Υπεύθυνο Παρακολούθησης Έργου ή το αρμόδιο τμήμα/γραφείο του Υπουργείου πριν την προσέλευση για εργασίες του προσωπικού του.

Ο ανάδοχος φέρει πλήρη ευθύνη για κάθε ζημία που προκαλείται από παραβίαση της Πολιτικής ή αμέλειά του, σύμφωνα με την κείμενη νομοθεσία.

3.2.9 ΥΠΟΧΡΕΩΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

- Οι ανάδοχοι έργου και οι συνεργάτες είναι υποχρεωμένοι να ειδοποιήσουν άμεσα το Τμήμα Υποδομών και Δικτύων του Υπουργείου Πολιτισμού για οποιοδήποτε περιστατικό

κυβερνοασφάλειας (data breach, malware, hacking, mail phising, μη εξουσιοδοτημένη πρόσβαση).

- Εφαρμογή ενημερώσεων/patches σε λογισμικό και συστήματα.
- Συμμόρφωση με ελέγχους ασφάλειας που ζητά το ΥΠΠΟ (penetration testing, audits).
- Χρήση μόνο εγκεκριμένου λογισμικού και εξοπλισμού.
- Να ενεργούν σύμφωνα με τις οδηγίες του Τμήματος Υποδομών και Δικτύων που είναι υπεύθυνο για την Κυβερνοασφάλεια.

Το Τμήμα Υποδομών και Δικτύων του Υπουργείου είναι υπεύθυνο να ελέγχει τις προσβάσεις των εξωτερικών συνεργατών σε τακτά χρονικά διαστήματα και να επιβεβαιώνει ή να αφαιρεί την πρόσβαση των χρηστών του αναδόχου/εξωτερικού συνεργάτη.

Η πρόσβαση των χρηστών του εξωτερικού συνεργάτη στα συστήματα του Υπουργείου χρειάζεται να είναι απενεργοποιημένη και να ενεργοποιείται από τους αρμόδιους υπαλλήλους του Τμήματος Υποδομών και Δικτύων όταν αυτοί επιβεβαιώνουν την ταυτότητα των χρηστών.

3.2.10 ΣΥΜΒΑΤΙΚΕΣ ΔΕΣΜΕΥΣΕΙΣ

Οι συμβάσεις με αναδόχους και συνεργάτες πρέπει να περιλαμβάνουν

- Ρήτρες προστασίας δεδομένων και εμπιστευτικότητας.
- Υποχρεώσεις συμμόρφωσης με πρότυπα και κανονισμούς ασφάλειας.
- Όρους για τον τερματισμό πρόσβασης σε περίπτωση λήξης ή παραβίασης της σύμβασης.
- Δικαιώματα ελέγχου και αξιολόγησης από τον οργανισμό.

Το Υπουργείο Πολιτισμού διατηρεί το δικαίωμα να διενεργεί ελέγχους συμμόρφωσης (audits) και να απαιτεί πιστοποιητικά ή αναφορές από ανεξάρτητους φορείς.

3.2.11 ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΑΙ ΕΛΕΓΧΟΣ

Το Υπουργείο Πολιτισμού, δύναται να παρακολουθεί, να ελέγχει και να αξιολογεί τη συμμόρφωση των τρίτων με την παρούσα Πολιτική και να επιβάλλει κυρώσεις σε περίπτωση παραβάσεων.

3.2.12 ΔΙΑΚΟΠΗ ΣΥΝΕΡΓΑΣΙΑΣ

Με τη λήξη ή καταγγελία της συνεργασίας:

- Όλες οι προσβάσεις ανακαλούνται άμεσα.
- Όλα τα δεδομένα, αντίγραφα ή assets που κατέχει ο ανάδοχος/συνεργάτης επιστρέφονται ή καταστρέφονται με ενδεδειγμένο τρόπο.
- Ο ανάδοχος/συνεργάτης υποχρεούται να παρέχει εγγράφως σχετική βεβαίωση καταστροφής/διαγραφής δεδομένων όπου απαιτείται.

3.2.13 ΑΝΑΘΕΩΡΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΠΟΛΙΤΙΚΗΣ

Διαχειριστής της υφιστάμενης Πολιτικής είναι ο Προϊστάμενος της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης, ο οποίος είναι υπεύθυνος για την εφαρμογή και την τήρησή της στο ΥΠΠΟ, καθώς και την αναθεώρησή της, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

- Σε περίπτωση σημαντικών αλλαγών στο ΥΠΠΟ.
- Σε περίπτωση περιστατικών ασφάλειας πληροφοριών ή κανονιστικών αλλαγών.
- Σε περίπτωση αλλαγών στο κανονιστικό πλαίσιο ISO/IEC 27001 ή στην εφαρμογή της NIS2
- Ετήσια αναθεώρηση με σκοπό τηβελτίωση της αποτελεσματικότητας της πολιτικής
- Ενημέρωσή της για αλλαγές στην τεχνολογία.

3.3 Πολιτική Ασφαλείας Υπηρεσιών Υπολογιστικού Νέφους

3.3.1 Εισαγωγή

Η χρήση υπηρεσιών νέφους (Cloud) αποτελεί πλέον αναπόσπαστο κομμάτι της λειτουργίας σύγχρονων οργανισμών, παρέχοντας ευελιξία, επεκτασιμότητα και βελτιστοποίηση πόρων. Ταυτόχρονα, η μετάβαση σε περιβάλλοντα Cloud εγείρει νέες προκλήσεις σε θέματα ασφάλειας και προστασίας δεδομένων. Η παρούσα πολιτική εισάγει το πλαίσιο και τις βασικές αρχές που καθοδηγούν το Υπουργείο στην ασφαλή αξιοποίηση των υπηρεσιών Cloud, διασφαλίζοντας τη συμμόρφωση με θεσμικές, κανονιστικές και τεχνικές απαιτήσεις.

3.3.2 Σκοπός

Η παρούσα πολιτική καθορίζει τις αρχές, τις απαιτήσεις και τις διαδικασίες που διέπουν τη χρήση, διαχείριση και προστασία υπηρεσιών νέφους (Cloud) στο Υπουργείο. Στόχος είναι η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων που φιλοξενούνται ή υποστηρίζονται σε περιβάλλοντα Cloud.

3.3.3 Πεδίο Εφαρμογής

Η πολιτική εφαρμόζεται σε:

- Όλους τους εργαζομένους, αναδόχους και συνεργάτες που χρησιμοποιούν υπηρεσίες Cloud για λογαριασμό του οργανισμού.
- Όλες τις κατηγορίες Cloud (IaaS, PaaS, SaaS).
- Όλα τα δεδομένα, εφαρμογές και υπηρεσίες που αποθηκεύονται, επεξεργάζονται ή διακινούνται μέσω Cloud.

3.3.4 Πολιτική

3.3.4.1 Επιλογή Παρόχων Cloud και Συμβατικές Υποχρεώσεις

Οι πάροχοι υπηρεσιών Cloud και οι σχετικές συμβάσεις συνεργασίας πρέπει να πληρούν τουλάχιστον τα ακόλουθα:

- Πιστοποίηση σε διεθνή πρότυπα (ISO 27001, ISO 27017/18, SOC 2).
- Κέντρα δεδομένων σε γεωγραφικές περιοχές που πληρούν τις νομικές απαιτήσεις (π.χ. GDPR).
- Όρους συμμόρφωσης με GDPR και άλλες σχετικές νομοθεσίες.
- Συμβατικές δεσμεύσεις εμπιστευτικότητας δεδομένων.
- Ρήτρες για την αναφορά περιστατικών ασφαλείας καθώς συνδρομής των παρόχων στην ανάλυση και αποκατάσταση περιστατικών.
- Υποχρέωση διαγρφής ή μεταφοράς δεδομένων σε ασφαλή μορφή μετά τη λήξη της συνεργασίας.

3.3.4.2 Αρχές Ασφάλειας

Η χρήση υπηρεσιών Cloud πρέπει να διέπεται από τις παρακάτω αρχές:

- Ελαχιστοποίηση πρόσβασης. Τα δικαιώματα χρήσης κάθε λογαριασμού περιορίζονται στο απολύτως αναγκαίο.

- Όλοι οι λογαριασμοί Cloud πρέπει να είναι ονομαστικοί.
- Χρήση πολυπαραγοντικής πιστοποίησης (MFA) για όλους τους διαχειριστές.
- Οι λογαριασμοί που δεν χρησιμοποιούνται πρέπει να απενεργοποιούνται άμεσα.
- Περιοδικοί έλεγχοι προσβάσεων.
- Κρυπτογράφηση δεδομένων κατά τη μεταφορά (in transit) και την αποθήκευση (at rest).
- Συμμόρφωση με κανονιστικά πλαίσια (GDPR, ISO 27017, ISO 27018).

3.3.4.3 Προστασία Δεδομένων

- Ευαίσθητα δεδομένα αποθηκεύονται μόνο σε περιβάλλοντα που υποστηρίζουν κρυπτογράφηση.
- Απαγορεύεται η αποθήκευση δεδομένων σε μη εγκεκριμένους Cloud παρόχους.
- Πρέπει να υλοποιούνται μηχανισμοί backup και disaster recovery.

3.3.4.4 Παρακολούθηση και Καταγραφή

- Όλες οι δραστηριότητες χρηστών και εφαρμογών σε Cloud υπηρεσίες πρέπει να καταγράφονται σε μορφή εγγραφών ελέγχου (logs) όπως ορίζει η πολιτική Παρακολούθησης και Καταγραφών Συμβάντων.
- Για τα κρίσιμα συστήματα, πρέπει να παρέχονται υπηρεσίες SIEM/monitoring για τον εντοπισμό ύποπτων δραστηριοτήτων οι οποίες να συνεργάζονται με τα συστήματα SIEM του Υπουργείου αν αυτό απαιτείται.
- Πρέπει να υπάρχει δυνατότητα διατήρησης των εγγραφών ελέγχου για τα χρονικά διαστήματα που απαιτεί κάθε σύστημα βάσει της αντίστοιχης πολιτικής Παρακολούθησης και Καταγραφών Συμβάντων.

3.3.5 Αναθεώρηση

Η πολιτική αναθεωρείται τουλάχιστον ετησίως ή νωρίτερα σε περίπτωση αλλαγών στο τεχνολογικό ή κανονιστικό πλαίσιο καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας.

3.4 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΚΑΤΑ ΤΟΝ ΣΧΕΔΙΑΣΜΟ – ΠΡΟΜΗΘΕΙΑ - ΑΝΑΠΤΥΞΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (SECURITY BY DESIGN / ACQUISITION & DEVELOPMENT POLICY)

3.4.1 ΕΙΣΑΓΩΓΗ

Το ΥΠΠΟ διαχειρίζεται, σε τακτική βάση, αιτήματα για νέα πληροφοριακά συστήματα και εφαρμογές, προκειμένου να υποστηρίζει αποτελεσματικά τις επιχειρησιακές λειτουργίες του.

Η πλειοψηφία, αν όχι το σύνολο, των πληροφοριακών συστημάτων και εφαρμογών που προμηθεύεται ή αναπτύσσει το ΥΠΠΟ επιδρούν σε πληροφορίες. Για το λόγο αυτό, κρίνεται σκόπιμη η υιοθέτηση μιας πολιτικής που θα καλύπτει τις πτυχές ασφάλειας πληροφοριών που σχετίζονται με την ανάπτυξη πληροφοριακών συστημάτων με ίδια μέσα, την ανάθεση της ανάπτυξης και διαχείρισης σε εξειδικευμένο εξωτερικό συνεργάτη, την προμήθεια εμπορικών συστημάτων / έτοιμων πακέτων λογισμικού και την ένταξη των παραπάνω σε λειτουργία και συντήρηση.

3.4.2 ΣΚΟΠΟΣ

Σκοπός της πολιτικής είναι:

- Ο σχεδιασμός, η κατάρτιση απαιτήσεων και τεχνικών προδιαγραφών ασφαλείας για την προμήθεια, την παρακολούθηση / εποπτεία, τη συντήρηση και τη διατήρηση της εύρυθμης και αδιάλειπτης λειτουργίας των νέων εφαρμογών και των πληροφοριακών συστημάτων.
- Η αποτροπή της απώλειας, της τροποποίησης ή της κακής χρήσης των δεδομένων στα πληροφοριακά συστήματα.
- Τα πληροφοριακών συστημάτων να λειτουργούν μέσω επίσημων διαδικασιών, σε όλη τη διάρκεια του κύκλου ζωής τους.
- Τα πληροφοριακά συστήματα να αξιολογούνται συνεχώς με βάση τις προδιαγραφές και τις απαιτήσεις ασφάλειας.
- Τα πληροφοριακά συστήματα, όταν δεν χρησιμοποιούνται πλέον, να αποσύρονται με εφαρμογή όλων των κατάλληλων μέτρων ασφάλειας.
- Την εξασφάλιση των δικτυακών και τηλεπικοινωνιακών υποδομών του ΥΠΠΟ.

3.4.3 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική ισχύει για τα στελέχη του ΥΠΠΟ, τους προμηθευτές, συμβούλους, αναδόχους κτλ. των οποίων τα εργασιακά καθήκοντα σχετίζονται με τον κύκλο ζωής των πληροφοριακών συστημάτων του ΥΠΠΟ και καλύπτει τις ακόλουθες δραστηριότητες που σχετίζονται με την προμήθεια, ανάπτυξη, υλοποίηση και διαχείριση συστημάτων:

- Εσωτερική ανάπτυξη και συντήρηση (δηλαδή ανάπτυξη με ίδια μέσα)
- Προμήθεια εμπορικών λύσεων / έτοιμων πακέτων λογισμικού

- Ανάθεση της ανάπτυξης και διαχείρισης σε εξειδικευμένο ανάδοχο/συνεργάτη (outsourcing)
- Λειτουργία και συντήρηση των πληροφοριακών συστημάτων με ίδια μέσα ή μέσω αναδόχων.

Η παρούσα πολιτική ενεργοποιείται στις εξής περιπτώσεις:

- Όταν η δραστηριότητα συνεπάγεται την ένταξη σε λειτουργία ενός υπολογιστικού συστήματος ή την ανάπτυξη ενός νέου πληροφοριακού συστήματος ή εφαρμογής ή module
- Όταν η δραστηριότητα περιλαμβάνει την προμήθεια ενός υπολογιστικού συστήματος, την οποία χειρίζεται το Τμήμα Υποδομών και Δικτύων ή άλλη αρμόδια οργανική μονάδα του ΥΠΠΟ.

3.4.4 ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΙΤΗΜΑΤΩΝ ΓΙΑ ΝΕΑ ΣΥΣΤΗΜΑΤΑ/ΕΦΑΡΜΟΓΕΣ

Το ΥΠΠΟ διαθέτει και χρησιμοποιεί μια τυπική, δομημένη και τεκμηριωμένη διαδικασία διαχείρισης αιτημάτων για νέα πληροφοριακά συστήματα / εφαρμογές.

Η διαδικασία αυτή περιλαμβάνει, κυρίως, τα ακόλουθα βήματα:

- Υποβολή αιτήματος νέου συστήματος / εφαρμογής από στέλεχος του ΥΠΠΟ στη Διεύθυνση Ηλεκτρονικής Διακυβέρνησης. Η υποβολή του αιτήματος αποτελεί το έναυσμα της διαδικασίας.
- Έλεγχος του αιτήματος από το αρμόδιο Τμήμα αναφορικά με την σκοπιμότητα / αναγκαιότητα του προτεινόμενου συστήματος / εφαρμογής σε συνάρτηση με τους επιχειρησιακούς στόχους και τις υπηρεσιακές ανάγκες του ΥΠΠΟ.
- Εφόσον το σύστημα / εφαρμογή κριθεί αναγκαίο/α, το αίτημα ανατίθεται σε αρμόδιο χειριστή.
- Ο αρμόδιος χειριστής ελέγχει τις λεπτομέρειες του αιτήματος και μεριμνά για τη διενέργεια ανάλυσης κόστους-οφέλους, ειδικά στα σημαντικότερα συστήματα. Ενδεικτικά, λαμβάνονται υπόψη, μεταξύ άλλων, η αύξηση της απόδοσης, η μείωση του λειτουργικού κόστους, καθώς και η δυνατότητα υλοποίησης, υποστήριξης και συντήρησης από πλευράς ανθρώπινου δυναμικού και λοιπών πόρων.
- Βάσει των αποτελεσμάτων της ανάλυσης κόστους–οφέλους, καθορίζεται ο τρόπος υλοποίησης του προτεινόμενου συστήματος / εφαρμογής. Η απόφαση αφορά την εκτέλεση του έργου με ίδια μέσα ή, εφόσον κρίνεται καταλληλότερο, την ανάθεση σε ανάδοχο, σύμφωνα με το ισχύον πλαίσιο.
- Στην περίπτωση που αποφασισθεί η ανάπτυξη με ίδια μέσα, τότε:
    - Ορίζονται στελέχη/ομάδα έργου, καταρτίζεται χρονοδιάγραμμα με τα παραδοτέα και ακολουθείται κατάλληλη μεθοδολογία ανάπτυξης συστημάτων. Αναλύονται οι απαιτήσεις δεδομένων και πλήθος συναλλαγών, ελέγχονται νέες/βελτιωμένες λύσεις πληροφορικής, εξετάζονται θέματα απορρήτου, ασφάλειας και κανονιστικών απαιτήσεων.

- Σχεδιάζεται μαζί με τον αιτούντα τόσο η ίδια η εφαρμογή όσο και η συνεργασία της με υφιστάμενα συστήματα. Η σχεδίαση εγκρίνεται από τους αρμόδιους Προϊστάμενους και ανάλογα με την περίπτωση από τρίτους, όπως τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO) και τον Υπεύθυνο Προστασίας Δεδομένων (DPO).
- Ακολουθούν, η υλοποίηση της εφαρμογής, οι δοκιμές και η διασφάλιση ποιότητας, η εκπαίδευση, η μετάπτωση δεδομένων από υφιστάμενα συστήματα στη νέα εφαρμογή και εφόσον κριθεί σκόπιμο, η δοκιμαστική / πιλοτική λειτουργία.
- Η νέα εφαρμογή εντάσσεται σε παραγωγική λειτουργία, δρομολογείται η παρακολούθησή και συντήρησή της και ολοκληρώνεται η διαδικασία.

- Στην περίπτωση που αποφασιστεί η ανάθεση σε ανάδοχο τότε:
  - Διαμορφώνονται οι τεχνικές προδιαγραφές από το αρμόδιο Τμήμα σε συνεργασία με τον αιτούντα.
  - Οι τεχνικές προδιαγραφές εγκρίνονται από τους αρμόδιους Προϊστάμενους και ανά περίπτωση από τρίτους, όπως από τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO), τον Υπεύθυνο Προστασίας Δεδομένων (DPO) κ.λπ.
  - Σκοπός είναι η προμήθεια αγαθών και υπηρεσιών που ικανοποιούν τις συγκεκριμένες επιχειρησιακές ανάγκες του ΥΠΠΟ, τα πρότυπα ασφαλείας και ιδιωτικότητας και παραλαμβάνονται στη σωστή ποιότητα, ποσότητα, τιμή και στον προγραμματισμένο χρόνο.
  - Οι προδιαγραφές αποστέλλονται στην αρμόδια υπηρεσία προμηθειών η οποία ακολουθεί τη διαδικασία της προμήθειας, που περιλαμβάνει αναζήτηση και επιλογή προμηθευτή/αναδόχου έργου, ανάθεση, σύναψη σύμβασης, παρακολούθηση και παραλαβή, σύμφωνα με το σχετικό νομοθετικό πλαίσιο περί δημοσίων συμβάσεων και η διαδικασία ολοκληρώνεται.

Κύριοι υπεύθυνοι για την παραπάνω διαδικασία είναι η Διεύθυνση Ηλεκτρονικής Διακυβέρνησης και η αρμόδια επιτροπή ή ομάδα, που συνεργάζονται στενά με τον υπηρεσιακό ιδιοκτήτη του συστήματος και τους τελικούς χρήστες ή άλλα εμπλεκόμενα μέρη.

3.4.5 ΑΝΑΛΥΣΗ ΑΠΑΙΤΗΣΕΩΝ ΚΑΙ ΚΑΘΟΡΙΣΜΟΣ ΠΡΟΔΙΑΓΡΑΦΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα πληροφοριακά συστήματα που προμηθεύεται ή αναπτύσσει το ΥΠΠΟ πρέπει να ανταποκρίνονται στις επιχειρησιακές ανάγκες και απαιτήσεις του. Για το σκοπό αυτό, σε κάθε περίπτωση, το ΥΠΠΟ ορίζει με σαφήνεια και λεπτομέρεια τις προδιαγραφές των νέων συστημάτων ως προς τη λειτουργικότητα και τα χαρακτηριστικά τους, τις υπηρεσίες και τις πληροφορίες που θα παρέχουν, την αρχιτεκτονική, τις τεχνολογίες υλοποίησης, τις απαιτήσεις διαλειτουργικότητας και ανταλλαγής δεδομένων με άλλα συστήματα, την παροχή ανοικτών δεδομένων, την ευχρηστία και φιλικότητα προς το χρήστη, την προσβασιμότητα, την επεκτασιμότητα και προσαρμοστικότητα στις μεταβαλλόμενες επιχειρησιακές ανάγκες, την ασφαλή λειτουργία, κ.λπ.

Παράλληλα, το ΥΠΠΟ ορίζει την επιθυμητή οργάνωση του έργου της εγκατάστασης /υλοποίησης κάθε νέου συστήματος, το χρονοδιάγραμμα, τις φάσεις, τα παραδοτέα και τα ορόσημα, καθώς και τις απαιτούμενες υπηρεσίες υποστήριξης, εγγύησης, συντήρησης κ.λπ.

3.4.6 ΑΝΑΛΥΣΗ - ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΩΝ

Τα πληροφοριακά συστήματα πρέπει να προστατεύονται από πρόσβαση ή τροποποίηση χωρίς εξουσιοδότηση, απώλεια της διαθεσιμότητάς τους ή απώλεια δεδομένων και άλλες απειλές, με τη χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας.

Τέτοια μέτρα μπορεί ενδεικτικά να περιλαμβάνουν τον καθορισμό των ρυθμίσεων ασφάλειας (παραμέτρων) του συστήματος, τη διαμόρφωση της δομής των απαραίτητων αρχείων καταγραφής (audit trails και logs) κ.λπ.

Πριν την προμήθεια ή ανάπτυξη του πληροφοριακού συστήματος και συγκεκριμένα πριν την οριστικοποίηση των προδιαγραφών ασφαλούς λειτουργίας του, διενεργείται ανάλυση κινδύνων.

Μέσω της ανάλυσης κινδύνων εντοπίζονται οι κίνδυνοι που δυνητικά αντιμετωπίζει το σύστημα, η πιθανότητα εμφάνισής τους και οι συνέπειές τους και εκτιμώνται οι απαιτήσεις ασφαλούς λειτουργίας του.

Έτσι προσδιορίζονται τα μέτρα ασφάλειας που πρέπει να εφαρμόζονται για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς του, σύμφωνα με όσα προβλέπει η Πολιτική Ασφαλείας του ΥΠΠΟ.

3.4.7 ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΠΡΟΔΙΑΓΡΑΦΕΣ ΩΣ ΠΡΟΣ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το ΥΠΠΟ ενσωματώνει απαιτήσεις και προδιαγραφές ασφάλειας πληροφοριών κατά την προκήρυξη, αξιολόγηση και προμήθεια συστημάτων, την ανάπτυξη με ίδια μέσα, την ανάθεση της ανάπτυξης σε τρίτους ή τις αναθεωρήσεις / αναβαθμίσεις των πληροφοριακών συστημάτων του. Οι συγκεκριμένες απαιτήσεις ασφάλειας διαφέρουν ανά σύστημα, διότι εξαρτώνται και επηρεάζονται από τα ειδικότερα χαρακτηριστικά του κάθε συστήματος, τους συγκεκριμένους επιχειρησιακούς στόχους του, τους τύπους δεδομένων που επεξεργάζεται (π.χ. προσωπικά δεδομένα), το επίπεδο ταξινόμησής του (κρίσιμο ή ευαίσθητο ή μη κρίσιμο σύμφωνα με τα οριζόμενα στην Πολιτική Διαχείρισης Πόρων), τα αποτελέσματα της ανάλυσης κινδύνων όπως αναφέρθηκε παραπάνω, τον επιτόπου ή εξ αποστάσεως έλεγχο/συντήρηση του συστήματος καθώς και το περιβάλλον στο οποίο το σύστημα θα εγκατασταθεί (π.χ. παραγωγής, ανάπτυξης, δοκιμών).

Επομένως, ανάλογα με τους παραπάνω παράγοντες, ένα νέο σύστημα ενδέχεται να προβλέπει προδιαγραφές για μηχανισμούς ελέγχου της πρόσβασης, τεχνικές κρυπτογράφησης ή άλλες μεθόδους προστασίας των δεδομένων, προστασία των συστημάτων μέσω λειτουργιών ελέγχου και καταγραφής (auditing και logging functions), κ.λπ.

Για παράδειγμα, στο σχεδιασμό εφαρμογών που αποθηκεύουν ή μεταδίδουν εμπιστευτικές

πληροφορίες, πρέπει να προβλέπονται αυξημένα μέτρα ασφάλειας για τον περιορισμό της πρόσβασης.

Στόχος σε κάθε περίπτωση είναι η ασφάλεια των πληροφοριακών συστημάτων σε επίπεδο ανάλογο με την κρισιμότητά τους και η προστασία έναντι των αυξανόμενων κινδύνων από κυβερνοεπιθέσεις (cyberesiliency).

Τονίζεται ότι η ασφάλεια των πληροφοριών λαμβάνεται υπόψη καθ' όλη τη διάρκεια του κύκλου ζωής ενός πληροφοριακού συστήματος, είτε αυτό αναπτύσσεται είτε προμηθεύεται, δηλαδή κατά την εκκίνηση του έργου ανάπτυξής του, την ανάλυση απαιτήσεων, το σχεδιασμό του συστήματος και την ανάπτυξη του λογισμικού ή αντίστοιχα, τον καθορισμό των τεχνικών προδιαγραφών, την επιλογή και αξιολόγηση των τρίτων μερών, την προμήθεια, καθώς επίσης, στις φάσεις της δοκιμής, της εγκατάστασης και της συντήρησης.

3.4.8 ΑΠΑΙΤΗΣΕΙΣ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

Στα κρίσιμα ή ευαίσθητα συστήματα πληροφοριών πρέπει να λαμβάνονται υπόψη και να εφαρμόζονται οι απαιτήσεις επιχειρησιακής συνέχειας (business continuity), δηλαδή οι δυνατότητες συνέχισης της λειτουργίας κατά την διάρκεια αντικατάστασης των συστημάτων ή αναβάθμισής των καθώς και μετά από μια καταστροφή και η δυνατότητα ανάκαμψης το συντομότερο δυνατόν.

3.4.9 ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΚΑΙ ΣΥΜΦΩΝΙΕΣ ΜΕ ΤΡΙΤΑ ΜΕΡΗ

Στην περίπτωση επιλογής τρίτων μερών, όπως προμηθευτών, αναδόχων, συμβούλων, κλπ., η επιλογή αυτή συμμορφώνεται με τη νομοθεσία περί δημοσίων συμβάσεων.

Από τεχνικής άποψης, κατά την επιλογή, θα πρέπει να αξιολογούνται η αξιοπιστία των συστημάτων, η καταλληλότητα και ωριμότητα των τεχνολογιών, οι παρεχόμενες υπηρεσίες (υποστήριξης, εκπαίδευσης, τεκμηρίωσης, εγγύησης, συντήρησης κτλ.), η πολιτική ασφάλειας και το σχέδιο συνέχειας εργασιών και ανάκαμψης από καταστροφή των υποψηφίων.

Οι προκηρύξεις των διαγωνισμών και οι συμβάσεις πρέπει να ενσωματώνουν τις απαιτήσεις του ΥΠΠΟ τόσο στη λήψη των συμφωνηθέντων αγαθών / υπηρεσιών όσο και στη διασφάλιση των πληροφοριών και της ιδιωτικότητας.

Πιο συγκεκριμένα, οι προμηθευτές-ανάδοχοι έργων-σύμβουλοι- κλπ τρίτα μέρη πρέπει μεταξύ άλλων να μεριμνούν σε συνεργασία με το Τμήμα Υποδομών και Δικτύων του ΥΠΠΟ για:

- Τη συμμόρφωση των συστημάτων με τα ισχύοντα πρότυπα ασφάλειας και ιδιωτικότητας και με τις απαιτήσεις του νομοθετικού και κανονιστικού πλαισίου που αναφέρθηκαν παραπάνω.
- Τη συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, ειδικά στην περίπτωση που το τρίτο μέρος λειτουργεί ως εκτελών επεξεργασία προσωπικών δεδομένων για λογαριασμό του ΥΠΠΟ.
- Τη συμμόρφωση με τις πολιτικές ασφαλείας του ΥΠΠΟ, π.χ. αναφορικά με την εξουσιοδοτημένη πρόσβαση, την ασφάλεια τελικού χρήστη, την προστασία προσωπικών

δεδομένων, την αποδεκτή χρήση των πληροφοριακών αγαθών, τη διαχείριση συμβάντων ασφαλείας κτλ.

- Τα θέματα που αφορούν τη μεθοδολογία (π.χ. μεθοδολογία ανάπτυξης πληροφοριακού συστήματος) και τις υπηρεσίες που θα παρέχουν κατά την υλοποίηση του έργου, ιδίως αναφορικά με τυχόν ιδιαίτερες απαιτήσεις που ενδεχομένως έχει το ΥΠΠΟ για ένα κρίσιμο ή ευαίσθητο σύστημα, όπως να εκτελεστεί δοκιμή διείσδυσης (penetration testing), δηλαδή προσομοίωση επίθεσης και εισβολής στο σύστημα, με σκοπό την επιβεβαίωση της ασφάλειάς του πριν την οριστική παραλαβή.
- Την ασφάλεια των διασυνδέσεων μεταξύ του ΥΠΠΟ και του τρίτου μέρους.
- Τα οργανωτικά και τεχνικά μέτρα ασφάλειας που λαμβάνουν και τις πιστοποιήσεις στην ασφάλεια πληροφοριών που κατέχουν.
- Το συμφωνηθέν επίπεδο παροχής υπηρεσιών (Service Level Agreement - SLA)
- Τα δικαιώματα ιδιοκτησίας και πνευματικών δικαιωμάτων και τα θέματα αδειοδότησης.
- Την συνεχή επιβεβαίωση από μέρους τους, της επάρκειας και ακεραιότητας του προσωπικού τους ως και της εμπιστευτικότητάς των.
- Την διαδικασία άμεσης αναφοράς στο ΥΠΠΟ των αδυναμιών ασφαλείας και των συμβάντων ασφαλείας που πιθανόν να εντοπίσει το τρίτο μέρος
- Τις διαδικασίες διαχείρισης αλλαγών του συστήματος τις οποίες υιοθετούν τα δύο μέρη.
- Το σχέδιο επικοινωνίας των δύο μερών (είδος, συχνότητα αναφορών / αρχείων κτλ.)
- Τα θέματα επιστροφής υλικού, λογισμικού, πληροφοριών και δεδομένων που ανήκουν στο ΥΠΠΟ μετά την ολοκλήρωση ή λύση της σύμβασης, καθώς και διαγραφής τυχόν αντιγράφων.

Κατά τη διάρκεια της σύμβασης, η συνεργασία του ΥΠΠΟ με το τρίτο μέρος διέπεται από τις σχετικές πολιτικές διαχείρισης τρίτων μερών του ΥΠΠΟ.

3.4.10 ΠΗΓΑΙΟΣ ΚΩΔΙΚΑΣ

Το ΥΠΠΟ πρέπει να εξετάζει το ενδεχόμενο σύναψης συμφωνιών μεσεγγύησης λογισμικού (software escrow) με τους εξωτερικούς συνεργάτες που της παρέχουν λύσεις λογισμικού.

Στη συμφωνία πρέπει να ορίζονται οι ενέργειες που πρέπει να υλοποιηθούν για την απελευθέρωση του πηγαίου κώδικα λογισμικού σε περιπτώσεις, στις οποίες ο αρχικός κάτοχος των πνευματικών δικαιωμάτων δεν είναι σε θέση να συντηρήσει και να αναβαθμίσει το λογισμικό, όπως έχει δεσμευτεί στη συμφωνία παραχώρησης άδειας χρήσης λογισμικού.

Σε τέτοιου είδους περιπτώσεις, ο πηγαίος κώδικας του λογισμικού πρέπει να φυλάσσεται σε λογαριασμό ανεξάρτητου μεσεγγυητή, ο οποίος φροντίζει για τη συντήρηση του λογισμικού.

Με τον τρόπο αυτό, προστατεύεται η επένδυση του ΥΠΠΟ σε επιχειρησιακά κρίσιμες εφαρμογές λογισμικού.

Η διαχείριση αλλαγών και ρυθμίσεων στον πηγαίο κώδικα συμμορφώνεται με την Πολιτική Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα του ΥΠΠΟ.

3.4.11 ΔΟΚΙΜΕΣ ΚΑΙ ΑΠΟΔΟΧΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ/ΕΦΑΡΜΟΓΩΝ

Το λογισμικό που αναπτύσσει ή προμηθεύεται το ΥΠΠΟ, καθώς και οι ενημερώσεις ή αναθεώρησης του, ελέγχεται πλήρως στο περιβάλλον δοκιμών και γίνεται αποδεκτό πριν από την εγκατάσταση στο περιβάλλον παραγωγής.

Θα πρέπει να γίνονται εκτεταμένες, τεκμηριωμένες και ολοκληρωμένες δοκιμές.

Οι δοκιμές ασφαλείας ελέγχουν ότι το σύστημα περιλαμβάνει τις δικλείδες ασφαλείας που προδιαγράφηκαν κατά τον σχεδιασμό του.

Οι δοκιμές αντοχής διενεργούνται σε συνθήκες επεξεργασίας αυξημένου όγκου δεδομένων και προσομοιώνουν ακραίες καταστάσεις.

Οι δοκιμές διαλειτουργικότητας επιβεβαιώνουν τη διαλειτουργικότητα του συστήματος με άλλα συστήματα.

Απαραίτητες είναι και οι δοκιμές για τον έλεγχο της δυνατότητας επαναφοράς του συστήματος σε περιπτώσεις βλάβης του λογισμικού ή του εξοπλισμού, κλπ.

Σε όλες τις περιπτώσεις, ο έλεγχος / η δοκιμή ασφαλείας που θα διενεργηθεί πριν από την εγκατάσταση του πληροφοριακού συστήματος, ενδείκνυται, ανάλογα και με την ταξινόμηση (κρισιμότητα / ευαισθησία) του συστήματος, να ανατίθεται σε μία ανεξάρτητη οντότητα (ανεξάρτητη ως προς την οντότητα υλοποίησης του συστήματος), προερχόμενη είτε από στελέχη του ΥΠΠΟ είτε ακόμη και από εξωτερικούς συνεργάτες.

Τα αποτελέσματα των δοκιμών διατηρούνται σύμφωνα με τις σχετικές πολιτικές.

Οι δοκιμές αποδοχής (acceptance tests) εκτελούνται με τρόπο ώστε να εξασφαλίζεται ότι τα πληροφοριακά συστήματα πληρούν τα καθορισμένα κριτήρια αποδοχής. Όλα τα κριτήρια αυτά πρέπει να πληρούνται πριν το οποιοδήποτε σύστημα ή εφαρμογή εγκατασταθεί σε περιβάλλον παραγωγής.

Στην περίπτωση που το νέο σύστημα αντικαθιστά παλαιότερο, συνιστάται να εξετάζεται η περίπτωση τα δύο συστήματα για ένα χρονικό διάστημα να λειτουργήσουν παράλληλα με τα ίδια δεδομένα και να αντιπαραβάλλονται τα αποτελέσματά τους.

3.4.12 ΤΕΚΜΗΡΙΩΣΗ – ΕΓΚΑΤΑΣΤΑΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ/ΕΦΑΡΜΟΓΩΝ

Κάθε πληροφοριακό σύστημα που αποκτάται από τρίτο μέρος ή αναπτύσσεται εσωτερικά στο ΥΠΠΟ, πρέπει να συνοδεύεται από πλήρη και ενημερωμένα εγχειρίδια (τεχνικά εγχειρίδια, εγχειρίδια διαχείρισης, χρήσης, λειτουργίας κ.λπ.).

Τα εγχειρίδια της τεκμηρίωσης θα πρέπει να έχουν ενιαία μορφή και δομή, όσο αυτό είναι δυνατόν.

Οι ιδιοκτήτες των πληροφοριακών συστημάτων είναι υπεύθυνοι για την ανάπτυξη και τήρηση ολοκληρωμένων εγχειριδίων.

Για να πραγματοποιηθεί η μετάβαση ενός πληροφοριακού συστήματος ή μιας εφαρμογής στο περιβάλλον παραγωγής, πρέπει να υπάρχει σχετική εισήγηση από το Τμήμα Υποδομών και Δικτύων του ΥΠΠΟ.

Η μετάβαση ενός πληροφοριακού συστήματος ή μιας εφαρμογής στο περιβάλλον παραγωγής εκτελείται μόνο από εξουσιοδοτημένο προσωπικό.

3.4.13 ΤΕΧΝΙΚΗ ΥΠΟΣΤΗΡΙΞΗ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟ ΤΡΙΤΑ ΜΕΡΗ

Οι περιπτώσεις στις οποίες απαιτείται υποστήριξη των συστημάτων του ΥΠΠΟ από τρίτα μέρη πρέπει να είναι σαφώς καθορισμένες, καθώς επίσης και ο τρόπος υποστήριξης από αυτά πρέπει να είναι αυστηρά προδιαγεγραμμένος και με συγκεκριμένα χρονικά περιθώρια ανταπόκρισής τους.

Οι περιπτώσεις απομακρυσμένης πρόσβασης αναδόχου στα συστήματα του ΥΠΠΟ για την επίλυση εκτάκτων προβλημάτων πρέπει να είναι περιορισμένες, να αντιμετωπίζονται με ιδιαίτερη προσοχή και σε κάθε περίπτωση να υπάρχει καταγραφή (logging) των ενεργειών του.

Όλα τα τρίτα μέρη είναι υποχρεωμένα να αναφέρουν στα αρμόδια στελέχη του τμήματος Υποδομών και Δικτύων του ΥΠΠΟ πιθανά προβλήματα σχετικά με τη λειτουργία των πληροφοριακών συστημάτων που υποπίπτουν στην αντίληψή τους.

3.4.14 ΑΝΑΘΕΩΡΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΠΟΛΙΤΙΚΗΣ

Ο διαχειριστής της υφιστάμενης Πολιτικής είναι ο Προϊστάμενος της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης, ο οποίος είναι υπεύθυνος για την εφαρμογή και την τήρησή της στο ΥΠΠΟ, καθώς και την αναθεώρησή της, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

- Σε περίπτωση σημαντικών αλλαγών στο ΥΠΠΟ.
- Σε περίπτωση περιστατικών ασφάλειας πληροφοριών.
- Ετήσια αναθεώρηση, εφόσον προκύπτει ανάγκη για:
    - Βελτίωση της αποτελεσματικότητας της πολιτικής
    - Ενημέρωσή της για αλλαγές στην τεχνολογία.

3.5 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΚΑΙ ΑΞΙΟΛΟΓΗΣΕΩΝ (Risk Management and Assessment Security Policy)

3.5.1 ΕΙΣΑΓΩΓΗ

Όλοι οι δημόσιοι φορείς, ανεξαρτήτως μεγέθους, δομής και αρμοδιοτήτων, έρχονται καθημερινά αντιμέτωποι με κινδύνους, σε όλα τα επίπεδα των δραστηριοτήτων τους.

Ως «κίνδυνος» (risk), σύμφωνα με το άρθρο 3 του ν. 4795/2021, ορίζεται «η πιθανότητα ή απειλή να επέλθει ζημία, απώλεια ή, γενικά, κάποια αρνητική συνέπεια για τους στόχους του φορέα, η οποία μπορεί να οφείλεται τόσο σε ενδογενείς, όσο και σε εξωγενείς παράγοντες και μπορεί να μετριαστεί μέσω προληπτικών δράσεων και δικλίδων ελέγχου».

Οι κίνδυνοι επομένως που αντιμετωπίζουν οι φορείς ενδέχεται να επιφέρουν αρνητικές επιπτώσεις στη λειτουργία τους όπως λανθασμένες στρατηγικές αποφάσεις, λειτουργικά σφάλματα, νομικές ευθύνες ή οικονομική αβεβαιότητα.

Με τον όρο «διαχείριση κινδύνων» αναφερόμαστε σε όλες τις δραστηριότητες που απαιτούνται για την αναγνώριση των κινδύνων που αντιμετωπίζει ο φορέας, την εκτίμηση (αξιολόγηση και ιεράρχηση), την αντιμετώπισή τους, καθώς και την παρακολούθηση και επικαιροποίησή τους.

3.5.2 ΔΗΜΙΟΥΡΓΙΑ ΚΟΥΛΤΟΥΡΑΣ ΚΙΝΔΥΝΟΥ

Η επίτευξη μιας αποτελεσματικής διαχείρισης κινδύνων εντός του φορέα, πέραν των ενεργειών που απαιτούνται για την υλοποίησή της, προϋποθέτει και την ανάπτυξη αντίστοιχης κουλτούρας. Η κουλτούρα κινδύνου αναφέρεται **«στις αξίες, τις πεποιθήσεις, τις γνώσεις, τις στάσεις και την κατανόηση σχετικά με τον κίνδυνο που μοιράζεται μια ομάδα ανθρώπων με κοινό σκοπό. Αυτό ισχύει για όλους τους οργανισμούς - συμπεριλαμβανομένων των φορέων του δημοσίου».**

Βασικές παράμετροι της κουλτούρας κινδύνου αποτελούν:

Υποστήριξη από τη Διοίκηση (tone at the top): Η διαχείριση κινδύνου πρέπει να υποστηρίζεται και να προωθείται από την ηγεσία, καθώς αυτό ενισχύει τη σημασία της σε όλο τον φορέα.

Λογοδοσία (Accountability): Το προσωπικό του φορέα, σε κάθε επίπεδο πρέπει να αναγνωρίζει την ευθύνη του για τη διαχείριση κινδύνων και οι αποφάσεις να λαμβάνονται με επίγνωση των κινδύνων. Για τον λόγο αυτό, οι ρόλοι του προσωπικού, καθώς και οι στόχοι της διαχείρισης κινδύνων πρέπει να είναι προσδιορισμένοι με σαφήνεια.

Ενσωμάτωση του Κινδύνου στη Στρατηγική: Η διαχείριση κινδύνων είναι μέρος της στρατηγικής σχεδίασης και της διαδικασίας λήψης αποφάσεων, σε όλα τα επίπεδα του φορέα.

Επικοινωνία: Υπάρχει διαφάνεια και ανοικτή επικοινωνία στον φορέα σχετικά με τους κινδύνους, καθώς και την αντιμετώπισή τους.

Ευαισθητοποίηση και Κατάρτιση: Το προσωπικό και η διοίκηση είναι ενημερωμένοι ή/και εκπαιδευμένοι σχετικά με τη σημασία και τις μεθόδους διαχείρισης κινδύνων. Προκειμένου

οι φορείς του δημόσιου τομέα να εξασφαλίσουν την ορθή λειτουργία και την ενσωμάτωση της διαχείρισης κινδύνων στις λειτουργίες τους, αναπτύσσουν και εφαρμόζουν Πολιτική και Πλαίσιο Διαχείρισης Κινδύνων.

3.5.3 ΜΕΡΟΣ 1ο

3.5.3.1 Πολιτική Διαχείρισης Κινδύνων

Η Πολιτική Διαχείρισης Κινδύνων καθοδηγεί τον φορέα στη λήψη αποφάσεων και ενεργειών που σχετίζονται με τη διαχείριση των κινδύνων στους οποίους είναι εκτεθειμένος. Στην Πολιτική περιγράφεται ο τρόπος διαχείρισης κινδύνων, ανά σκοπό και στόχο, η διάθεση ανάληψης και το επίπεδο ανοχής κινδύνου, καθώς και οι ρόλοι και οι αρμοδιότητες των κατάλληλων επιπέδων διοίκησης, σε σχέση με τον σχεδιασμό, την παρακολούθηση και την εφαρμογή του Πλαισίου διαχείρισης κινδύνων.

Επισημαίνεται ότι η διαχείριση κινδύνων δεν αποτελεί μία διακριτή διαδικασία/λειτουργία εντός του φορέα, αλλά πρέπει να συνιστά αναπόσπαστο μέρος της κουλτούρας όλων των οργανικών μονάδων, αντικατοπτρίζοντας τον τρόπο με τον οποίο λειτουργεί και αντιμετωπίζει τις προκλήσεις ο φορέας. Η Πολιτική Διαχείρισης Κινδύνων θα πρέπει κατ' ελάχιστο να διαρθρώνεται από τις παρακάτω ενότητες με το αντίστοιχο περιεχόμενο:

3.5.3.1.1 ΣΚΟΠΟΣ

Ο σκοπός της **Πολιτικής Ασφάλειας Διαχείρισης Κινδύνων** είναι να καθορίσει το πλαίσιο, τις αρχές και τις διαδικασίες που εφαρμόζονται για τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση και την παρακολούθηση των κινδύνων που σχετίζονται με την ασφάλεια πληροφοριών και τις επιχειρησιακές λειτουργίες του οργανισμού.

Πιο συγκεκριμένα, η Πολιτική Διαχείρισης Κινδύνων του ΥΠΠΟ στοχεύει στα εξής :

- Εξασφάλιση της εμπιστευτικότητάς, ακεραιότητας και διαθεσιμότητας των πληροφοριών.
- Οι κίνδυνοι αναγνωρίζονται εγκαίρως και αξιολογούνται με συστηματικό και τεκμηριωμένο τρόπο.
- Εφαρμόζονται κατάλληλα μέτρα ελέγχου και μετριασμού των κινδύνων, ανάλογα με το επίπεδο απειλής και την ανοχή του οργανισμού σε κίνδυνο (risk appetite).
- Διατηρείται ένα συνεπές και αποδοτικό σύστημα διαχείρισης κινδύνων που υποστηρίζει τη λήψη τεκμηριωμένων αποφάσεων και ενισχύει την ανθεκτικότητα του οργανισμού.
- Εξασφαλίζεται η συμμόρφωση με κανονιστικές, νομικές και συμβατικές υποχρεώσεις σχετικά με τη διαχείριση κινδύνων και την ασφάλεια πληροφοριών.

3.5.3.1.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η Πολιτική Ασφάλειας Διαχείρισης Κινδύνων εφαρμόζεται σε:

- Όλα τα πληροφοριακά συστήματα, υπηρεσίες και υποδομές του οργανισμού που εμπλέκονται στην επεξεργασία, αποθήκευση, ή διακίνηση πληροφοριών.
- Όλο το προσωπικό του οργανισμού, ανεξαρτήτως ρόλου ή θέσης, καθώς και σε εξωτερικούς συνεργάτες, προμηθευτές και τρίτα μέρη που έχουν πρόσβαση σε πληροφορίες ή συστήματα του οργανισμού.

- Όλες τις μορφές πληροφοριών που είναι ηλεκτρονικές και αποθηκευμένες σε οποιοδήποτε μέσο.

3.5.3.1.3 ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

Η διαχείριση κινδύνων δεν επαφίεται αποκλειστικά στο όργανο διαχείρισης κινδύνων. Αντίθετα, απαιτεί τη συμμετοχή όλου του προσωπικού του φορέα. Από τον επικεφαλής του φορέα, τα ανώτατα στελέχη της Διοίκησης (Γενικοί Γραμματείς, Γενικοί Διευθυντές, κ.λπ.), το όργανο διαχείρισης κινδύνων έως τους Διευθυντές και τους υπαλλήλους, καθώς και τα τρίτα μέρη (ανάδοχοι, εξωτερικοί συνεργάτες), όλοι συμβάλλουν στη δημιουργία ενός περιβάλλοντος, όπου η αποτελεσματική διαχείριση των κινδύνων μπορεί να ευδοκιμήσει. Για τον λόγο αυτό, η διαχείριση κινδύνων απαιτεί σαφή προσδιορισμό των ρόλων και των αρμοδιοτήτων του προσωπικού σε όλα τα επίπεδα. Στην ενότητα αυτή, περιγράφονται οι ρόλοι και οι αρμοδιότητες τόσο του επικεφαλής του φορέα και των ανώτερων ιεραρχικών στελεχών αυτού, όσο και των υπαλλήλων, σε σχέση με τη διαχείριση κινδύνων.

Πιο συγκεκριμένα:

● **Ο επικεφαλής του φορέα είναι υπεύθυνος για:**

α) τον καθορισμό της διάθεσης ανάληψης κινδύνου, καθώς και τον καθορισμό της ανοχής κινδύνου του φορέα,

β) την έγκριση της Πολιτικής και του Πλαισίου Διαχείρισης Κινδύνων του φορέα και τη διασφάλιση της συμμόρφωσης του φορέα με την Πολιτική και το Πλαίσιο Διαχείρισης Κινδύνων του ΥΠΠΟ,

γ) την ενσωμάτωση της διαδικασίας διαχείρισης κινδύνων στις λειτουργίες του φορέα και την παροχή υπηρεσιών,

δ) την εφαρμογή στρατηγικών διαχείρισης κινδύνων για την αντιμετώπιση των κινδύνων του φορέα,

ε) την κατά προτεραιότητα αντιμετώπιση των πολύ υψηλών (ακραίων) κινδύνων για τους στόχους και τη λειτουργία του φορέα,

στ) κάθε άλλη ενέργεια που απορρέει από το υφιστάμενο θεσμικό πλαίσιο, αναφορικά με τη διαχείριση κινδύνων και τη λειτουργία του Μητρώου κινδύνων (όπως έγκριση μέτρων αντιμετώπισης κινδύνων, εισαγωγή νέων κινδύνων στο Μητρώο κ.λπ.).

● **Ο Υπεύθυνος διαχείρισης κινδύνων είναι αρμόδιος για:**

την εκτέλεση των αρμοδιοτήτων του, όπως περιγράφονται στο άρθρο 22Δ του ν. 4795/2021,

και ειδικότερα:

α) την εισήγηση της Πολιτικής Διαχείρισης Κινδύνων προς τον επικεφαλής του φορέα,

β) την ανάπτυξη, παρακολούθηση και επικαιροποίηση του Πλαισίου Διαχείρισης Κινδύνων του φορέα, σύμφωνα με τους στρατηγικούς και επιχειρησιακούς στόχους του,

γ) την ενημέρωση και καθοδήγηση του προσωπικού του φορέα, σχετικά με τον τρόπο εντοπισμού και αντιμετώπισης των κινδύνων, κατά την άσκηση των αρμοδιοτήτων του και την παρακολούθηση των δικλίδων ελέγχου,

δ) την εποπτεία της διαδικασίας διαχείρισης κινδύνων που διενεργείται από το σύνολο των οργανικών μονάδων του φορέα,

ε) την τήρηση, τη συνεχή παρακολούθηση και την επικαιροποίηση του Μητρώου Κινδύνων του φορέα και την παροχή κατευθύνσεων προς τις λοιπές οργανικές μονάδες,

στ) την υποβολή περιοδικών και έκτακτων αναφορών προς τον επικεφαλής του φορέα, σχετικά με τους κινδύνους στους οποίους είναι εκτεθειμένος ο φορέας και

- **Οι υπάλληλοι είναι υπεύθυνοι για:**

α) τη συμμόρφωση με τις πολιτικές, τις διαδικασίες και τις κατευθυντήριες γραμμές του φορέα για τη διαχείριση κινδύνων,

β) την παρακολούθηση της εφαρμογής των δικλίδων ελέγχου, στο πεδίο ευθύνης τους και την αναφορά περιστατικών μη εφαρμογής ή πλημμελούς εφαρμογής αυτών, στους άμεσα προϊσταμένους τους,

γ) τον εντοπισμό των πιθανών κινδύνων κατά την άσκηση των καθημερινών αρμοδιοτήτων τους και την αναφορά αυτών στους άμεσα προϊσταμένους τους.

3.5.3.1.4 ΚΑΤΗΓΟΡΙΕΣ ΚΙΝΔΥΝΟΥ

3.5.3.1.4.1 Κίνδυνοι Ασφάλειας Πληροφοριών

- Παραβίαση δεδομένων (data breach) – Μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες.
- Κακόβουλο λογισμικό (malware, ransomware, trojans) – Καταστροφή ή μπλοκάρισμα δεδομένων.
- Απώλεια δεδομένων (data loss) – Από λάθος, τεχνική αστοχία ή κυβερνοεπίθεση.
- Ανεπαρκής έλεγχος πρόσβασης – Παροχή δικαιωμάτων σε μη εξουσιοδοτημένα άτομα.
- Ανεπαρκής κρυπτογράφηση – Επιτρέπει υποκλοπή ευαίσθητων πληροφοριών.

3.5.3.1.4.2 Κίνδυνοι Διαθεσιμότητας και Συνέχειας Λειτουργίας

- Βλάβες συστημάτων ή υποδομών (π.χ. διακοπή ρεύματος, αστοχία hardware).
- Μη ύπαρξη εφεδρικών (backup) ή σχεδίων ανάκαμψης (disaster recovery plans).
- Επιθέσεις άρνησης υπηρεσίας (DDoS).
- Ανεπαρκής φυσική ασφάλεια (π.χ. ζημιές σε data centers).

3.5.3.1.4.3 Κίνδυνοι Συμμόρφωσης και Νομικοί Κίνδυνοι

- Παραβίαση GDPR ή άλλων νόμων περί προστασίας δεδομένων.
- Παραβίαση πνευματικών δικαιωμάτων ή συμβάσεων με τρίτους.
- Μη συμμόρφωση με πρότυπα ασφαλείας (ISO 27001, PCI DSS, NIS2 κ.λπ.).

3.5.3.1.4.4. Κίνδυνοι Ανθρώπινου Παράγοντα

- Ανθρώπινα λάθη στη διαχείριση δεδομένων.
- Ανεπαρκής εκπαίδευση ή ευαισθητοποίηση προσωπικού.
- Εσωτερικές απειλές (insider threats).
- Ανεπαρκής διαδικασία εισόδου/εξόδου προσωπικού (onboarding/offboarding).

3.5.3.1.4.5. Κίνδυνοι Τεχνολογικής Εξέλιξης και Τεχνικών Εξαρτήσεων

• Παρωχημένο λογισμικό χωρίς ενημερώσεις ασφαλείας.

• Εξάρτηση από τρίτους παρόχους IT (cloud, outsourcing).

• Ανεπαρκής διαχείριση αλλαγών (change management).

• Ασυμβατότητα νέων τεχνολογιών με υπάρχουσες υποδομές.

3.5.3.1.4.6. Κίνδυνοι Διακυβέρνησης και Διαχείρισης

• Απουσία πλαισίου διαχείρισης κινδύνων.

• Ανεπαρκής παρακολούθηση δεικτών ασφάλειας (security KPIs).

• Μη αποτελεσματική επικοινωνία ή έλλειψη λογοδοσίας**.**

3.5.3.2 ΔΙΑΘΕΣΗ ΑΝΑΛΗΨΗΣ ΚΙΝΔΥΝΟΥ(Risk Appetite)

Όλοι οι φορείς κατά τη λειτουργία τους αντιμετωπίζουν τόσο εσωτερικούς όσο και εξωτερικούς κινδύνους, τους οποίους δεν μπορούν να εξαλείψουν πλήρως και ως εκ τούτου θα πρέπει να τους διαχειριστούν, προκειμένου να επιτύχουν τους στόχους τους, ενώ θα υπάρξουν και κίνδυνοι, τους οποίους θα αποδεχθούν. Ως Διάθεση Ανάληψης Κινδύνου ορίζεται «το είδος και το μέγεθος του κινδύνου που ένας φορέας είναι διατεθειμένος να επιδιώξει ή να διατηρήσει14», προκειμένου να επιτύχει τους στόχους του. Η δήλωση Διάθεσης Ανάληψης Κινδύνου, η οποία εγκρίνεται από τον επικεφαλής, εκφράζει πόσο διατεθειμένος είναι ένας φορέας να αναλάβει τους κινδύνους (το «ρίσκο») που προκύπτουν από την υλοποίηση των στόχων του, διασφαλίζοντας μια ισορροπημένη σχέση μεταξύ επιδιωκόμενου οφέλους και δυνητικού ρίσκου. Η Διάθεση Ανάληψης Κινδύνου μπορεί να διατυπώνεται και ανά κατηγορία κινδύνου, έτσι όπως οι κατηγορίες αναλύονται στην προηγούμενη ενότητα, ακολουθώντας την παρακάτω κλίμακα. Αυτή η προσέγγιση επιτρέπει την εστίαση σε κάθε κατηγορία ξεχωριστά, αξιολογώντας και αντιμετωπίζοντας τους κινδύνους με τον πλέον αποτελεσματικό τρόπο.

3.5.3.3 ΑΝΟΧΗ ΚΙΝΔΥΝΟΥ (Risk tolerance)

Στην ενότητα αυτή, ορίζεται η ανοχή κινδύνου ανά κατηγορία κινδύνου. Ως ανοχή κινδύνου ορίζεται «η ετοιμότητα ενός οργανισμού ή ενός ενδιαφερόμενου μέρους να αναλάβει τον κίνδυνο που απομένει, μετά τα μέτρα που λαμβάνονται για αντιμετώπισή του, προκειμένου να επιτύχει τους στόχους του». Με τον όρο αυτόν επομένως, δηλώνεται ένα επίπεδο απόκλισης από τη διάθεση ανάληψης κινδύνου που ένας φορέας είναι διατεθειμένος να αναλάβει. Κατά συνέπεια, η ανοχή κινδύνου μπορεί να ορισθεί ως ένα συγκεκριμένο και προκαθορισμένο εύρος απόκλισης από τη διάθεση ανάληψης κινδύνου.

Επισημαίνεται ότι η ανοχή κινδύνου ενίοτε περιορίζεται από θεσμικές και κανονιστικές ρυθμίσεις, όπως οι νομοθετικές απαιτήσεις για την υγεία και την ασφάλεια. Η ανοχή κινδύνου μπορεί να αφορά υποκατηγορίες κινδύνων ή μεμονωμένους κινδύνους, συγκεκριμένα έργα, επί μέρους στόχους, πρωτοβουλίες κ.λπ., έτσι ώστε να λαμβάνονται υπόψη οι ιδιαιτερότητες που εμφανίζει κάθε κίνδυνος, έργο ή περιοχή κινδύνου (υποκατηγορία). Για την ενιαία εφαρμογή των διατάξεων του ν. 4795/2021, οι φορείς θα πρέπει να εφαρμόζουν τη διαβάθμιση της διάθεσης ανάληψης κινδύνου, όπως αποτυπώνεται στο παρόν κείμενο.

3.5.4 ΜΕΡΟΣ 2ο

3.5.4.1 ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΙΝΔΥΝΟΥ

3.5.4.1.1 ΣΚΟΠΟΣ ΜΕΘΟΔΟΛΟΓΙΑΣ

Η μεθοδολογία αξιολόγησης κινδύνου καθορίζει τον τρόπο με τον οποίο ο οργανισμός εντοπίζει, αναλύει, αξιολογεί και διαχειρίζεται τους κινδύνους που σχετίζονται με την ασφάλεια πληροφοριών και τις επιχειρησιακές λειτουργίες του. Αποσκοπεί στη δημιουργία ενός **συνεκτικού, τεκμηριωμένου και επαναλαμβανόμενου πλαισίου** που επιτρέπει την αντικειμενική λήψη αποφάσεων σχετικά με τον χειρισμό κάθε κινδύνου.

3.5.4.1.2 ΒΑΣΙΚΕΣ ΑΡΧΕΣ

Η διαδικασία αξιολόγησης κινδύνου στηρίζεται στις εξής αρχές:

- **Συστηματικότητα και τεκμηρίωση:** Όλα τα στάδια πρέπει να είναι επαναλήψιμα και καταγεγραμμένα.
- **Αντικειμενικότητα:** Η εκτίμηση κινδύνου βασίζεται σε αποδεικτικά στοιχεία, δεδομένα και αντικειμενικά κριτήρια.
- **Αναλογικότητα:** Η προσέγγιση προσαρμόζεται στο μέγεθος, τη φύση και το προφίλ κινδύνου του οργανισμού.
- **Συμμετοχικότητα:** Εμπλέκονται οι υπεύθυνοι από όλα τα τμήματα που σχετίζονται με τα υπό αξιολόγηση στοιχεία.
- **Συνεχής βελτίωση:** Η μεθοδολογία επανεξετάζεται περιοδικά για να ενσωματώνει νέες απειλές, τεχνολογίες ή κανονιστικές απαιτήσεις.

3.5.4.1.3 ΚΑΤΑΓΡΑΦΗ ΑΠΕΙΛΩΝ ΚΑΙ ΤΡΩΤΟΤΗΤΩΝ

Η διαδικασία αξιολόγησης κινδύνου στηρίζεται στις εξής αρχές:

- Χρήση καταλόγων απειλών (π.χ. ENISA, ISO/IEC 27005, OWASP).
- Καταγραφή πιθανών τρωτοτήτων (τεχνικών, οργανωτικών, φυσικών).
- Σύνδεση απειλών–τρωτοτήτων με επιχειρησιακά περιουσιακά στοιχεία (assets).

3.5.4.1.4 ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΠΛΑΙΣΙΟΥ (Context Establishment)

Σε αυτό το στάδιο καθορίζονται:

- Τα όρια και το πεδίο εφαρμογής της αξιολόγησης κινδύνου.
- Οι στόχοι της αξιολόγησης (π.χ. συμμόρφωση με ISO 27001, προστασία δεδομένων, επιχειρησιακή συνέχεια).
- Οι κατηγορίες περιουσιακών στοιχείων (assets) που θα αξιολογηθούν: πληροφορίες, λογισμικό, υλικό, δίκτυα, προσωπικό, εγκαταστάσεις, διαδικασίες.
- Οι υποχρεώσεις που απορρέουν από νόμους, κανονισμούς και συμβάσεις.

3.5.4.1.5 ΚΑΤΑΓΡΑΦΗ ΑΠΕΙΛΩΝ ΚΑΙ ΤΡΩΤΟΤΗΤΩΝ

Στόχος είναι ο εντοπισμός όλων των πιθανών απειλών και ευπαθειών που μπορεί να επηρεάσουν τα στοιχεία του οργανισμού.

- Χρήση καταλόγων απειλών (π.χ. ENISA, ISO/IEC 27005, OWASP).
- Απειλές (Threats): Εξωτερικές ή εσωτερικές ενέργειες που μπορούν να προκαλέσουν ζημία (π.χ. κακόβουλο λογισμικό, φυσικές καταστροφές, ανθρώπινα λάθη).
- Ευπάθειες (Vulnerabilities): Αδυναμίες που μπορούν να αξιοποιηθούν από απειλές (π.χ. μη ενημερωμένα συστήματα, ανεπαρκής εκπαίδευση).
- Περιουσιακά Στοιχεία (Assets): Οτιδήποτε έχει αξία για τον οργανισμό (δεδομένα, υποδομές, εφαρμογές, φήμη).
- Πιθανές Επιπτώσεις (Impacts): Οι συνέπειες που θα έχει η πραγματοποίηση του κινδύνου (π.χ. οικονομική ζημία, νομικές κυρώσεις, απώλεια εμπιστοσύνης).

Όλα τα παραπάνω καταγράφονται σε Μητρώο Κινδύνων (Risk Register).

3.5.4.1.5 ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ (Risk Analysis)

Η ανάλυση στοχεύει στον ποσοτικό ή ποιοτικό υπολογισμό του επιπέδου κινδύνου, με βάση δύο κύριες μεταβλητές:

• Πιθανότητα (Likelihood): Η πιθανότητα να συμβεί ένα περιστατικό.

• Επίπτωση (Impact): Η σοβαρότητα των συνεπειών εάν συμβεί.

Η εκτίμηση γίνεται συνήθως με κλίμακες (π.χ. 1–5 ή "Χαμηλή–Μέτρια–Υψηλή") και χρησιμοποιείται ο τύπος:

Κίνδυνος = Πιθανότητα × Επίπτωση

Ανάλογα με τη μεθοδολογία, μπορεί να περιλαμβάνονται και παράγοντες όπως:

- Έκθεση σε απειλές (exposure)
- Εντοπισιμότητα / ανίχνευση
- Υπολειπόμενος κίνδυνος (residual risk)

3.5.4.1.7 ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΩΝ (Risk Evaluation)

Σε αυτό το στάδιο συγκρίνονται τα αποτελέσματα της ανάλυσης με κριτήρια αποδοχής κινδύνου (risk acceptance criteria).

Οι κίνδυνοι κατηγοριοποιούνται ως:

- Αποδεκτοί: Δεν απαιτούν περαιτέρω ενέργεια.
- Ανεκτοί με έλεγχο: Χρειάζονται μέτρα μετριασμού ή παρακολούθησης.
- Μη αποδεκτοί: Απαιτούν άμεση παρέμβαση ή ανασχεδιασμό διαδικασιών.

3.5.4.1.8 ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΙΝΔΥΝΩΝ (Risk Treatment)

Για κάθε μη αποδεκτό κίνδυνο, καθορίζονται και εφαρμόζονται ενέργειες αντιμετώπισης:

1. Αποδοχή (Accept) – Ο οργανισμός αποδέχεται τον κίνδυνο εντός καθορισμένων ορίων.
2. Μείωση (Mitigate) – Εφαρμόζονται τεχνικά ή οργανωτικά μέτρα για τη μείωση πιθανότητας ή επιπτώσεων.
3. Μεταφορά (Transfer) – Ο κίνδυνος μεταφέρεται σε τρίτο (π.χ. ασφάλιση, outsourcing).
4. Αποφυγή (Avoid) – Διακοπή δραστηριότητας ή αλλαγή διαδικασίας ώστε να εξαλειφθεί ο κίνδυνος.

Για κάθε απόφαση τεκμηριώνονται οι υπεύθυνοι, τα χρονοδιαγράμματα και τα μέσα παρακολούθησης.

3.5.4.1.9 ΣΧΕΔΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ (Mitigation Plans)

Για κάθε μη αποδεκτό κίνδυνο, καθορίζονται και εφαρμόζονται ενέργειες αντιμετώπισης:

• Περιγραφή μέτρου (τεχνικού, οργανωτικού, εκπαιδευτικού).

• Υπεύθυνος εφαρμογής.

• Χρονοδιάγραμμα.

• Δείκτες επιτυχίας (KPIs).

3.5.4.1.10 ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΑΙ ΑΝΑΘΕΩΡΗΣΗ (Monitoring & Review)

Για κάθε μη αποδεκτό κίνδυνο, καθορίζονται και εφαρμόζονται ενέργειες αντιμετώπισης:

• Περιοδική επανεκτίμηση (π.χ. ετήσια ή μετά από σημαντικές αλλαγές).

• Αναθεώρηση καταλόγου απειλών–τρωτοτήτων.

• Αξιολόγηση αποτελεσματικότητας υλοποιημένων μέτρων.

3.5.4.1.11 ΤΕΚΜΗΡΙΩΣΗ ΚΑΙ ΑΝΑΦΟΡΑ

Όλα τα στάδια, τα δεδομένα και οι αποφάσεις τεκμηριώνονται και φυλάσσονται με ασφάλεια.

Η τεκμηρίωση περιλαμβάνει:

• Πλαίσιο και πεδίο εφαρμογής της ανάλυσης.

• Πίνακα απειλών, ευπαθειών, επιπτώσεων και μέτρων.

• Risk register με βαθμολογήσεις και υπεύθυνους.

• Αξιολόγηση αποτελεσματικότητας υλοποιημένων μέτρων.

• Αναφορές προς τη Διοίκηση για λήψη αποφάσεων.

ΠΑΡΑΡΤΗΜΑ 4.1: Καταγραφή_Απειλών_και_Τρωτοτήτων_με_Αξιολόγηση (excel)

ΠΑΡΑΡΤΗΜΑ 4.2: Εργαλείο_Αξιολόγησης_Κινδύνου_με_Φίλτρα_και_DropDown (excel)

ΠΑΡΑΡΤΗΜΑ 4.3: Risk_Register_Template (excel)

ΠΑΡΑΡΤΗΜΑ 4.4: Risk_Treatment_Plan (excel)

ΠΑΡΑΡΤΗΜΑ 4.5: Risk Appetite & Tolerance Policy (Word)

3.6 Πολιτική Ανοχής σε Κίνδυνο (Risk Appetite & Tolerance Policy)

3.6.1. Σκοπός

Η παρούσα πολιτική καθορίζει τα αποδεκτά επίπεδα κινδύνου που ο οργανισμός είναι διατεθειμένος να αναλάβει κατά τη λειτουργία του, ώστε να διασφαλίζεται ισορροπία μεταξύ προστασίας, επιχειρησιακής συνέχειας και αποδοτικότητας.

3.6.2. Πεδίο Εφαρμογής

Η πολιτική ισχύει για όλους τους τομείς του οργανισμού, περιλαμβανομένων:
- των πληροφοριακών συστημάτων και της ασφάλειας δεδομένων,
- των επιχειρησιακών διαδικασιών,
- των ανθρώπινων πόρων,
- και των σχέσεων με τρίτους (προμηθευτές, συνεργάτες, πελάτες).

3.6.3. Ορισμοί

• Όρεξη για Κίνδυνο (Risk Appetite): Το γενικό επίπεδο κινδύνου που ο οργανισμός αποδέχεται στο πλαίσιο επίτευξης των στόχων του.

• Ανοχή σε Κίνδυνο (Risk Tolerance): Τα επιμέρους αποδεκτά όρια κινδύνου ανά κατηγορία ή δραστηριότητα.

3.6.4. Αρχές Πολιτικής

1. Οι κίνδυνοι αξιολογούνται με βάση την πιθανότητα εμφάνισης και την επίπτωσή τους σε κρίσιμα στοιχεία (π.χ. διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα).
2. Οι αποφάσεις λαμβάνονται βάσει του Risk Matrix, το οποίο ορίζει ποιοι κίνδυνοι είναι ανεκτοί, υπό όρους ή μη αποδεκτοί.
3. Η ανοχή σε κίνδυνο επανεξετάζεται τουλάχιστον μία φορά τον χρόνο ή όταν αλλάζουν οι επιχειρησιακές συνθήκες.

3.6.5. Καθορισμός Επίπεδων Ανοχής

Επίπεδο Κινδύνου	Περιγραφή	Ανοχή	Ενέργεια
Χαμηλό	Μικρή πιθανότητα και περιορισμένες επιπτώσεις	Αποδεκτός	Δεν απαιτούνται πρόσθετα μέτρα
Μεσαίο	Μέτρια πιθανότητα ή επίπτωση	Υπό όρους ανεκτός	Λήψη μέτρων μετριασμού και παρακολούθηση
Υψηλό	Υψηλή πιθανότητα ή σημαντική επίπτωση	Μη ανεκτός	Άμεση αντιμετώπιση – αποφυγή ή μεταφορά
Πολύ Υψηλό	Κίνδυνοι που απειλούν τη φήμη, τη συμμόρφωση ή τη λειτουργία του οργανισμού	Μη αποδεκτός	Άμεση αποφυγή, διακοπή δραστηριότητας ή κρίσιμη απόφαση Διοίκησης

3.6.6. Ειδικά Όρια Ανοχής

- Ασφάλεια πληροφοριών: Καμία παραβίαση εμπιστευτικών δεδομένων δεν είναι ανεκτή.
- Διαθεσιμότητα συστημάτων: Μέγιστη ανεκτή διακοπή (Maximum Tolerable Downtime – MTD) = 4 ώρες.
- Οικονομικές απώλειες: Ανεκτές απώλειες έως 1% του ετήσιου προϋπολογισμού ανά περιστατικό.
- Κανονιστική συμμόρφωση: Μηδενική ανοχή σε μη συμμόρφωση με νομικές ή κανονιστικές απαιτήσεις.

3.6.7. Ευθύνες

- Η Ανώτατη Διοίκηση εγκρίνει και αναθεωρεί το επίπεδο ανοχής.
- Η Ομάδα Διαχείρισης Κινδύνων / Πληροφορικής Ασφάλειας παρακολουθεί την εφαρμογή.
- Οι Υπεύθυνοι Τμημάτων διασφαλίζουν ότι οι λειτουργίες τους παραμένουν εντός των αποδεκτών ορίων κινδύνου.

3.6.8. Αναθεώρηση Πολιτικής

Η πολιτική αναθεωρείται ετησίως ή όποτε μεταβληθεί σημαντικά το επιχειρησιακό ή τεχνολογικό περιβάλλον.

3.7 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΑΥΤΟΤΗΤΑΣ & ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

3.7.1 ΣΚΟΠΟΣ

Η παρούσα πολιτική καθορίζει τις αρχές και τις διαδικασίες για τη διαχείριση ταυτότητας χρηστών και τον έλεγχο πρόσβασης στα πληροφοριακά συστήματα, δίκτυα και εφαρμογές του Υπουργείου Πολιτισμού. Στόχος είναι να εξασφαλιστεί ότι:

- κάθε χρήστης έχει μοναδική και επαληθεύσιμη ταυτότητα,
- η πρόσβαση περιορίζεται μόνο όπου απαιτείται για την εκτέλεση καθηκόντων,
- διατηρείται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών.

3.7.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική εφαρμόζεται σε:

- όλους τους υπαλλήλους, συνεργάτες και εξωτερικούς αναδόχους,
- όλα τα πληροφοριακά συστήματα, δίκτυα, εφαρμογές και βάσεις δεδομένων του Υπουργείου,
- κάθε μέσο πρόσβασης (υπολογιστές, κινητά, tablets, VPN, cloud υπηρεσίες).

3.7.3 ΟΡΙΣΜΟΙ

Ταυτότητα (Identity): μοναδικό αναγνωριστικό ενός χρήστη (π.χ. username).
Έλεγχος Πρόσβασης (Access Control): οι μηχανισμοί που επιτρέπουν ή απαγορεύουν την πρόσβαση σε πληροφοριακούς πόρους.
Αρχή της Ελάχιστης Αναγκαίας Πρόσβασης (Least Privilege): κάθε χρήστης έχει μόνο τα δικαιώματα που απαιτούνται για τα καθήκοντά του.
MFA (Multi-Factor Authentication): έλεγχος ταυτότητας με περισσότερους από έναν παράγοντες.

3.7.4 ΑΡΧΕΣ ΠΟΛΙΤΙΚΗΣ

1.Αρχές Ελέγχου.

- Δεν δημιουργείται κανένας λογαριασμός χωρίς τεκμηριωμένη υπηρεσιακή ανάγκη και έγκριση
- Απαγορεύεται η δημιουργία “γενικών” ή “ανώνυμων” λογαριασμών
- Οι κωδικοί είναι προσωπικοί και μη μεταβιβάσιμοι
- Η ευθύνη της ορθότητας του αιτήματος για τη δημιουργία λογαριασμού χρήστη σε πληροφοριακά συστήματα του Υπουργείου Πολιτισμού ανήκει στην υπηρεσία προέλευσης

2. Μοναδική Ταυτότητα Χρήστη. Κάθε χρήστης διαθέτει προσωπικό λογαριασμό. Απαγορεύεται η κοινή χρήση λογαριασμών.

3. Έγκριση Πρόσβασης. Όλες οι προσβάσεις εγκρίνονται από το Τμήμα Υποδομών και Δικτύων και τον Υπεύθυνο Ασφάλειας Πληροφοριών.

4. Διαχωρισμός Καθηκόντων. Οι ρόλοι χρηστών διαχωρίζονται ώστε να αποτρέπεται η σύγκρουση συμφερόντων.

5. Πολυπαραγοντικός Έλεγχος (MFA). Ενεργοποιείται όπου υποστηρίζεται, ιδίως για την απομακρυσμένη πρόσβαση και διαχειριστικούς λογαριασμούς.

6. Αναθεώρηση Πρόσβασης. Οι προσβάσεις επανεξετάζονται τουλάχιστον ανά εξάμηνο από το Τμήμα Υποδομών και Δικτύων.

7. Απενεργοποίηση Λογαριασμών. Οι λογαριασμοί απενεργοποιούνται άμεσα με τη λήξη σύμβασης ή αποχώρηση υπαλλήλου.

3.7.5 ΔΙΑΔΙΚΑΣΙΑ ΑΠΟΚΤΗΣΗΣ ΛΟΓΑΡΙΑΣΜΟΥ ΧΡΗΣΤΗ

Η διαδικασία αυτή καθορίζει τα βήματα για τη δημιουργία, έγκριση και ενεργοποίηση υπηρεσιακού λογαριασμού χρήστη σε πληροφοριακά συστήματα του Υπουργείου Πολιτισμού, ώστε να εξασφαλίζεται ότι κάθε λογαριασμός εκδίδεται μόνο με επίσημη έγκριση και τεκμηριωμένη υπηρεσιακή ανάγκη.

3.7.5.1 Αρμόδιοι Φορείς

- Υπηρεσία Προέλευσης Χρήστη: Η υπηρεσία όπου υπηρετεί ο/η υπάλληλος. Είναι υπεύθυνη να πιστοποιήσει την ανάγκη πρόσβασης και να υποβάλει το σχετικό αίτημα.
- Τμήμα Υποδομών και Δικτύων: Διαχειρίζεται τη δημιουργία, παραμετροποίηση και ενεργοποίηση λογαριασμών.
- Υπεύθυνος Ασφάλειας Πληροφοριών: Διασφαλίζει ότι η διαδικασία τηρείται και ότι εφαρμόζονται οι αρχές της ασφάλειας πληροφοριών (π.χ. Least Privilege, MFA).
- Υπεύθυνος Προστασίας Δεδομένων (DPO), όπου απαιτείται: Σε περιπτώσεις που η πρόσβαση αφορά δεδομένα προσωπικού χαρακτήρα ή ευαίσθητα δεδομένα.

3.7.5.2 Διαδικασία

Βήμα	**Περιγραφή**	**Υπεύθυνος**
Αίτημα Πρόσβασης	Υποβολή αιτήματος μέσω υπηρεσιακού email ή ticketing system. Η υπηρεσία του υπαλλήλου υποβάλλει επίσημο αίτημα δημιουργίας λογαριασμού, αναφέροντας: – Ονοματεπώνυμο υπαλλήλου – Α.Μ. / email επικοινωνίας – Θέση και καθήκοντα	Προϊστάμενος Υπηρεσίας προέλευσης χρήστη

	– Συστήματα ή εφαρμογές στα οποία απαιτείται πρόσβαση	
Έγκριση	Έλεγχος αιτήματος και έγκριση. Το Τμήμα Υποδομών και Δικτύων ελέγχει το αίτημα, επιβεβαιώνει ότι προέρχεται από εξουσιοδοτημένο αποστολέα και εγκρίνει τη δημιουργία του λογαριασμού στο σύστημα. Ο Υπεύθυνος Ασφάλειας Πληροφοριών εγκρίνει την τελική χορήγηση πρόσβασης εξασφαλίζοντας είναι σύμφωνη με τις πολιτικές ασφάλειας. Όπου η πρόσβαση αφορά δεδομένα προσωπικού χαρακτήρα ή ευαίσθητα δεδομένα, ενημερώνεται και ο DPO.	Τμήμα Υποδομών και Δικτύων και Υπεύθυνος Ασφάλειας Πληροφοριών
Δημιουργία Λογαριασμού	Εγκατάσταση, καταγραφή και ενεργοποίηση. Το Τμήμα Υποδομών και Δικτύων δημιουργεί τον λογαριασμό με μοναδικό αναγνωριστικό χρήστη (username) και αποδίδει προσωρινό κωδικό. Όλες οι λεπτομέρειες (όνομα, ρόλος, ημερομηνία δημιουργίας, σύστημα πρόσβασης) καταγράφονται στο Μητρώο Διαχείρισης Πρόσβασης.	Τμήμα Υποδομών και Δικτύων
Ενημέρωση Χρήστη	Ο χρήστης ενημερώνεται για την ενεργοποίηση του λογαριασμού μέσω απάντησης στο Αίτημα Πρόσβασης (υπηρεσιακού email ή ticketing system).	Τμήμα Υποδομών και Δικτύων και Υπηρεσία προέλευσης χρήστη
Είσοδος και ενεργοποίηση MFA	Ο χρήστης υποχρεούται να: - ρυθμίσει το MFA (όπου απαιτείται), – αλλάξει τον προσωρινό κωδικό κατά την πρώτη είσοδο	Χρήστης
Αναθεώρηση	Έλεγχος ορθότητας και ανανέωση δικαιωμάτων	Τμήμα Υποδομών και Δικτύων
Απενεργοποίηση	Αυτόματη ή χειροκίνητη κατάργηση	Τμήμα Υποδομών και Δικτύων

3.7.5.3 ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

- Τουλάχιστον 12 χαρακτήρες, με γράμματα, αριθμούς και σύμβολα.

- Ανανέωση κάθε 180 ημέρες.
- Απαγορεύεται η αποθήκευση ή κοινοποίηση κωδικών σε μη ασφαλή μέσα.

3.7.6 ΠΡΟΣΒΑΣΗ ΤΡΙΤΩΝ & ΑΝΑΔΟΧΩΝ

Οι εξωτερικοί συνεργάτες, ανάδοχοι ή προμηθευτές που αποκτούν πρόσβαση σε πληροφοριακά συστήματα, δεδομένα ή δίκτυα του Υπουργείου Πολιτισμού, υπόκεινται στους ίδιους κανόνες ασφάλειας με τους υπαλλήλους του Υπουργείου, καθώς και στις ακόλουθες πρόσθετες απαιτήσεις:

1. Περιορισμένη Πρόσβαση. Η πρόσβαση παρέχεται μόνο στα απολύτως απαραίτητα συστήματα και δεδομένα, σύμφωνα με τους όρους της σύμβασης ή του έργου.

2. Έλεγχος Ταυτότητας με MFA. Όλοι οι τρίτοι χρήστες υποχρεούνται να χρησιμοποιούν Πολυπαραγοντικό Έλεγχο Ταυτότητας (Multi-Factor Authentication) για την πρόσβαση σε οποιοδήποτε σύστημα ή υπηρεσία του Υπουργείου, είτε μέσω τοπικού δικτύου είτε απομακρυσμένα (VPN, cloud, web portal).

3. Συμφωνία Εμπιστευτικότητας (NDA). Κάθε εξωτερικός χρήστης υπογράφει Ρήτρα Εμπιστευτικότητας και Αποδοχής Όρων Ασφάλειας Πληροφοριών πριν αποκτήσει πρόσβαση.

4. Χρονικός Περιορισμός. Οι λογαριασμοί τρίτων είναι προσωρινοί, με ημερομηνία λήξης που δεν υπερβαίνει τη διάρκεια του έργου ή της σύμβασης.

5. Έλεγχος και Καταγραφή. Όλες οι ενέργειες των τρίτων χρηστών καταγράφονται (audit logs) και υπόκεινται σε έλεγχο από το Τμήμα Ασφάλειας Πληροφοριών.

6. Απενεργοποίηση Πρόσβασης. Με τη λήξη της συνεργασίας ή του έργου, οι λογαριασμοί απενεργοποιούνται άμεσα και τα δικαιώματα ανακαλούνται.

3.7.7 Αναθεώρηση

Η πολιτική αναθεωρείται ετησίως ή νωρίτερα, όταν απαιτείται, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

- Σε περίπτωση σημαντικών αλλαγών στην υποδομή
- Σε περίπτωση περιστατικών ασφάλειας
- Εφόσον προκύπτει ανάγκη για ενημέρωσή της για αλλαγές στην τεχνολογία

3.8 Πολιτική Διαχείρισης Τρωτοτήτων & Ενημερώσεων

3.8.1 Εισαγωγή

Η ασφάλεια των πληροφοριακών συστημάτων αποτελεί θεμελιώδη προϋπόθεση για την απρόσκοπτη λειτουργία, την αξιοπιστία και την προστασία των δεδομένων ενός οργανισμού. Σε ένα περιβάλλον συνεχών τεχνολογικών αλλαγών και αυξανόμενων κυβερνοαπειλών, απαιτείται η εφαρμογή οργανωμένων διαδικασιών που διασφαλίζουν τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών. Ως εκ τούτου είναι αναγκαία η συστηματική ανίχνευση ευπαθειών στα υφιστάμενα πληροφοριακά συστήματα και η τεκμηριωμένη εφαρμογή διορθωτικών ενεργειών.

3.8.2 Σκοπός

Η παρούσα πολιτική καθορίζει τις αρχές και τις διαδικασίες που ακολουθεί το Υπουργείο για την έγκαιρη αναγνώριση, αξιολόγηση και διόρθωση ευπαθειών στα Πληροφοριακά και Επικοινωνιακά Συστήματά του. Στόχος είναι η μείωση του κινδύνου από κακόβουλες επιθέσεις, η διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών και η συμμόρφωση με διεθνή πρότυπα και κανονιστικά πλαίσια.

3.8.3 Πεδίο Εφαρμογής

Η πολιτική αφορά:

- Όλα τα ΠΕΣ του Υπουργείου όπως αυτά καταγράφονται στο Μητρώο Πληροφοριακών Συστημάτων καθώς και όλα τα τερματικά.
- Όλο το προσωπικό (εσωτερικό και εξωτερικούς συνεργάτες) που εμπλέκεται στη διαχείριση και υποστήριξη συστημάτων.

3.8.4 Πολιτική

Η διαδικασία διαχείρισης τρωτοτήτων και ενημερώσεων αναλύεται σε 5 στάδια: Αναγνώριση, Καταγραφή, Έγκριση, Υλοποίηση και Επαλήθευση.

3.8.4.1 Αναγνώριση

Σε τακτική βάση, οι υπεύθυνοι των ΠΕΣ λαμβάνουν και επεξεργάζονται πληροφορίες που αφορούν σε τεχνικές ευπάθειες και ενημερώσεις ασφαλείας των συστημάτων τους, μέσω κατάλληλων πηγών, όπως:

- αρμόδιες αρχές,
- ερευνητικοί οργανισμοί,
- προμηθευτές και πάροχοι υπηρεσιών (software/firmware updates),
- αρμόδιες ομάδες απόκρισης σε περιστατικά κυβερνοασφάλειας (CSIRTs) όπως η Εθνική Αρχή Κυβερνοασφάλειας.

Σε ετήσια βάση ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας, διενεργείται αυτοαξιολόγηση της ασφάλειας των ΠΕΣ η οποία περιλαμβάνει:

- Χαρτογράφηση της υποδομής με εργαλεία ιχνηλάτισης.
    - Αναγνώριση και απαρίθμηση δικτύων.
    - Καθορισμός περιμετρικής υποδομής.

- Καθορισμός συνολικών συστημάτων υπό εξέταση.

- Έλεγχος συστημάτων.
  - Καταγραφή λειτουργικού συστήματος ή firmware που χρησιμοποιείται.
  - Καταγραφή ενεργών υπηρεσιών, σκοπού χρήσης και εκδόσεων των σχετικών λογισμικών.
  - Καταγραφή γνωστών ευπαθειών και διαθέσιμων ενημερώσεων ασφαλείας.
- Σάρωση ευπαθειών μέσω αυτοματοποιημένων εργαλείων.

Σε ετήσια βάση ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας, διενεργείται εξωτερικός έλεγχος παρείσδυσης στα συστήματα δικτύου και πληροφοριών.

3.8.4.2 Καταγραφή

Κάθε ευπάθεια, που προκύπτει κατά το στάδιο της Αναγνώρισης, καταγράφεται και αξιολογείται εφαρμόζοντας το σύστημα βαθμολογίας CVSS 3.1 και λαμβάνοντας υπόψη τον επιχειρησιακό αντίκτυπο. Βάσει της αξιολόγησης αυτής κατατάσσονται σε 4 κατηγορίες:

- **Κρίσιμη (Critical):** Βαθμολογία CVSS ≥ 9.0 ή ευπάθεια που ενέχει άμεσο και σοβαρό κίνδυνο για κρίσιμα πληροφοριακά συστήματα ή/και ευαίσθητα δεδομένα του οργανισμού.
- **Υψηλή (High):** Βαθμολογία CVSS 7.0–8.9 ή ευπάθεια που μπορεί να αξιοποιηθεί με σημαντικό δυνητικό αντίκτυπο στη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα των πληροφοριών.
- **Μεσαία (Medium):** Βαθμολογία CVSS 4.0–6.9 ή ευπάθεια με μέτριο αντίκτυπο ή περιορισμένες συνθήκες εκμετάλλευσης, η οποία ενδέχεται να απαιτεί τοπική πρόσβαση ή αλληλεπίδραση χρήστη.
- **Χαμηλή (Low):** Βαθμολογία CVSS ≤ 3.9 ή ευπάθεια μικρού ή πληροφοριακού χαρακτήρα, με ελάχιστο ή θεωρητικό κίνδυνο για τα συστήματα.

3.8.4.3 Έγκριση

Οι υπεύθυνοι των ΠΕΣ αναλύουν τις ευπάθειες που προκύπτουν από το στάδιο Καταγραφής και:

- καθορίζουν τις σχετικές ενημερώσεις ασφαλείας ή/και τροποποιήσεις που πρέπει να υλοποιηθούν,
- αποφασίζουν αν απαιτείται έγκριση από τους ιδιοκτήτες των συστημάτων,
- αποφασίζουν αν απαιτούνται δοκιμαστικές υλοποιήσεις σε ελεγχόμενο περιβάλλον,
- καθορίζουν το χρονοδιάγραμμα υλοποίησης.

Τα χρονικά περιθώρια αποκατάστασης κάθε ευπάθειας εξαρτώνται από την κατηγοριοποίησή τους:

- **Κρίσιμη (Critical):** Εντός 24 - 72 ωρών.
- **Υψηλή (High):** Εντός 7 ημερών.

- **Μεσαία (Medium):** Εντός 30 ημερών.
- **Χαμηλή (Low):** Εντός 90 ημερών.

Σε περίπτωση που κάποια ενημέρωση ασφαλείας δεν υφίσταται τη δεδομένη στιγμή, ή δεν μπορεί να εφαρμοστεί λόγω λειτουργικών περιορισμών, ή τα μειονεκτήματα της εφαρμογής της υπερτερούν έναντι των πλεονεκτημάτων στην ασφάλεια πληροφοριών, ορίζονται κατάλληλα αντισταθμιστικά μέτρα προστασίας ή αποφασίζεται η αποδοχή του ρίσκου. Σε κάθε περίπτωση τηρείται πλήρης τεκμηρίωση για κάθε τέτοια απόφαση.

3.8.4.4 Υλοποίηση

Οι υπεύθυνοι των ΠΕΣ υλοποιούν τις εγκεκριμένες ενημερώσεις ασφαλείας βάσει του δοθέντος χρονοδιαγράμματος. Για κάθε υλοποίηση πρέπει να υπάρχει η δυνατότητα επαναφοράς των συστημάτων στην πρότερη κατάσταση σε περίπτωση αποτυχίας. Η επιτυχημένη ή αποτυχημένη υλοποίηση καταγράφεται συμπεριλαμβάνοντας όποια πληροφορία μπορεί να θεωρηθεί χρήσιμη για μελλοντικές ενέργειες.

3.8.4.5 Επαλήθευση

Η επιτυχημένη υλοποίηση των ενημερώσεων επαληθεύεται με κάθε πρόσφορο μέσο όπως ο επανέλεγχος των εκδόσεων των λογισμικών ή η εκ νέου διενέργεια σάρωσης ευπαθειών.

3.8.4.6 Αναθεώρηση

Η πολιτική αναθεωρείται τουλάχιστον ετησίως ή νωρίτερα σε περίπτωση αλλαγών στο τεχνολογικό ή κανονιστικό πλαίσιο καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας.

3.9 ΠΟΛΙΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

3.9.1 ΣΚΟΠΟΣ

Η πολιτική αυτή καθορίζει το πλαίσιο και τις αρχές για την εφαρμογή της κρυπτογράφησης (encryption) ως οριζόντιου μέτρου ασφάλειας στο Υπουργείο Πολιτισμού.
Η υιοθέτηση κρυπτογράφησης είναι κρίσιμη για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, καθώς η απουσία της αποτελεί κοινή αιτία για περιστατικά Διαρροής Δεδομένων (Data Breach).

3.9.2 ΣΥΝΔΕΣΗ ΜΕ ΣΥΜΜΟΡΦΩΣΗ

Η υιοθέτηση κρυπτογράφησης συνδέεται άμεσα με τη συμμόρφωση του Υπουργείου στις απαιτήσεις του Υπευθύνου Προστασίας Δεδομένων (DPO) και του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR-Κανονισμός ΕΕ 2016/679).

Η υλοποίηση αυτής της πολιτικής μειώνει σημαντικά τον κίνδυνο απώλειας ή μη εξουσιοδοτημένης αποκάλυψης προσωπικών και ευαίσθητων δεδομένων.

3.9.3 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική αυτή ισχύει για:

- Όλους τους υπαλλήλους, συνεργάτες και αναδόχους που διαχειρίζονται ή αποθηκεύουν δεδομένα του Υπουργείου.
- Όλα τα πληροφοριακά συστήματα, δίκτυα, συσκευές αποθήκευσης (NAS/SAN), laptops, φορητά μέσα, cloud υπηρεσίες και ηλεκτρονικές επικοινωνίες του Υπουργείου Πολιτισμού.

Όλα τα δεδομένα του Υπουργείου που χαρακτηρίζονται ως εμπιστευτικά, προσωπικά ή διαβαθμισμένα

3.9.4 ΑΡΧΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

1. Η κρυπτογράφηση εφαρμόζεται σε όλα τα επίπεδα, ως οριζόντιο μέτρο ασφάλειας.
2. Χρησιμοποιούνται μόνο εγκεκριμένοι (από NIST ή ENISA) αλγόριθμοι και πρωτόκολλα:
    - Συμμετρική κρυπτογράφηση: AES-256
    - Ασύμμετρη κρυπτογράφηση: RSA-2048 ή υψηλότερο
    - Hashing: SHA-256 ή ανώτερο
3. Όλα τα ευαίσθητα δεδομένα αποθηκεύονται ή διακινούνται μόνο μέσω κρυπτογραφημένων διαύλων.
4. Η πολιτική ισχύει εξίσου για δεδομένα σε ηρεμία (at rest) και σε μεταφορά (in transit).

3.9.5 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ

Υποχρεωτική ενεργοποίηση κρυπτογράφησης σε όλα τα NAS/SAN, servers και φορητές συσκευές.
Τα αποθηκευτικά μέσα πρέπει να προστατεύονται με πλήρη κρυπτογράφηση δίσκου (Full

Disk Encryption) ή τεχνολογίες native encryption του κατασκευαστή. Όλα τα δεδομένα που διακινούνται μέσω δικτύων ή internet πρέπει να προστατεύονται με TLS 1.2+, VPN ή S/MIME για email.

3.9.6 Διαχείριση Κλειδιών (Key Management)

Η διαχείριση των κλειδιών κρυπτογράφησης γίνεται με ασφάλεια και τεκμηριωμένα:

- Δημιουργία και αποθήκευση κλειδιών σε ασφαλές περιβάλλον, (π.χ. HSM ή KMS).
- Περιορισμένη πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό.
- Ανανεώσεις κλειδιών ανά 2 έτη και ασφαλής καταστροφή μετά τη λήξη ισχύος.
- Τήρηση μητρώου κλειδιών και σχετικών ενεργειών.
- Ανάκληση & καταστροφή: με τη λήξη ισχύος ή αλλαγή υπευθύνου, τα παλιά κλειδιά καταστρέφονται με ασφάλεια.

3.9.7 Χρήση Κρυπτογράφησης σε Εφαρμογές & Επικοινωνίες

- Υποχρεωτική χρήση HTTPS, S/MIME ή PGP για αποστολή ευαίσθητων μηνυμάτων
- Εσωτερικά APIs πρέπει να χρησιμοποιούν mutual TLS
- Οι βάσεις δεδομένων που αποθηκεύουν προσωπικά δεδομένα πρέπει να έχουν ενεργοποιημένη encryption-at-rest.

3.9.8 Φορητές Συσκευές & Αφαιρούμενα Μέσα

- Όλα τα φορητά μέσα αποθήκευσης πρέπει να είναι κρυπτογραφημένα με BitLocker ή ισοδύναμη τεχνολογία.
- Σε περίπτωση απώλειας συσκευής, ενεργοποιείται διαδικασία συμβάντος ασφάλειας.

3.9.10 Ευθύνες

- Τμήμα Υποδομών και Δικτύων: Υλοποίηση, παρακολούθηση και διαχείριση της κρυπτογράφησης.
- DPO (Υπεύθυνος Προστασίας Δεδομένων): Εξασφαλίζει τη συμμόρφωση με τον GDPR και παρακολουθεί περιστατικά διαρροής.
- Όλοι οι χρήστες: Υποχρεούνται να χρησιμοποιούν μόνο εγκεκριμένα μέσα και εργαλεία.

3.9.11 Εκπαίδευση & Ευαισθητοποίηση

Όλοι οι χρήστες λαμβάνουν περιοδική εκπαίδευση για:

- Τη σωστή χρήση κρυπτογραφημένων μέσων.
- Τον ασφαλή χειρισμό κλειδιών ή πιστοποιητικών.
- Την αναφορά περιστατικών απώλειας ή αποκάλυψης κρυπτογραφικών στοιχείων.

3.9.12 Παρακολούθηση & έλεγχος

Η συμμόρφωση με την παρούσα πολιτική παρακολουθείται μέσω:
- Τακτικών ελέγχων εφαρμογής κρυπτογράφησης σε συστήματα και μέσα.
- Επιθεωρήσεων ISMS (ISO 27001) και GDPR audit reports.
- Ελέγχου των NAS/SAN για ενεργή κρυπτογράφηση at rest.

Τα ευρήματα τεκμηριώνονται και διορθωτικές ενέργειες λαμβάνονται άμεσα.

Συσχετισμός με ISO 27001:

Κωδικός Ελέγχου	**Περιγραφή**	**Εφαρμογή στην Πολιτική**
A.5.28	Protection of information using cryptography (Προστασία πληροφοριών με κρυπτογράφηση)	Καθορισμός απαιτήσεων χρήσης κρυπτογράφησης για δεδομένα και επικοινωνίες.
A.5.29	Key management (Διαχείριση Κλειδιών)	Διαχείριση, αποθήκευση και ανάκληση κλειδιών κρυπτογράφησης.
A.5.30	Use of cryptographic controls (Χρήση ελέγχων κρυπτογράφησης)	Επιλογή και χρήση εγκεκριμένων αλγορίθμων και πρωτοκόλλων.

3.9.13 Εξαιρέσεις

Οποιαδήποτε εξαίρεση στην παρούσα πολιτική απαιτεί εγκεκριμένη αιτιολόγηση και έγκριση από τον Υπεύθυνο Ασφάλειας Πληροφοριών.

3.9.14 Αναθεώρηση

Η πολιτική αναθεωρείται ετησίως ή νωρίτερα, όταν απαιτείται, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

- Σε περίπτωση σημαντικών αλλαγών στην υποδομή
- Σε περίπτωση περιστατικών ασφάλειας
- Εφόσον προκύπτει ανάγκη για ενημέρωσή της για αλλαγές στην τεχνολογία

3.10 Πολιτική Παρακολούθησης και Καταγραφής Συμβάντων

3.10.1 Εισαγωγή

Προκειμένου να εφαρμοστούν οι πολιτικές ελέγχου προσβάσεων και τα μέτρα ασφάλειας, πρέπει να διατηρούνται, τόσο χειροκίνητα όσο και αυτοματοποιημένα, αρχεία καταγραφής προσβάσεων και αλλαγών στα Πληροφοριακά και Επικοινωνιακά Συστήματα (ΠΕΣ) του Υπουργείου καθώς και τα τερματικά. Για κάθε σύστημα διατηρούνται ένα ή περισσότερα αρχεία εγγραφών ελέγχου δραστηριότητας των χρηστών και των εφαρμογών. Από κοινού με τα κατάλληλα εργαλεία και τις διαδικασίες, οι εγγραφές ελέγχου μπορούν να βοηθήσουν στην ανίχνευση των παραβιάσεων ασφάλειας, των προβλημάτων απόδοσης και των ελαττωμάτων στις εφαρμογές.

3.10.2 Σκοπός

Σκοπός της πολιτικής αυτής είναι η συστηματική καταγραφή και διατήρηση εγγραφών ελέγχου για όλα τα ΠΕΣ του Υπουργείου καθώς και τα τερματικά. Στόχος είναι η απόδοση ευθύνης για τη χρήση των παραπάνω πόρων καθώς και η αποτελεσματική διερεύνηση περιστατικών κυβερνοασφάλειας.

3.10.3 Πεδίο Εφαρμογής

Η πολιτική αφορά:

- Όλα τα ΠΕΣ του Υπουργείου όπως αυτά καταγράφονται στο Μητρώο Πληροφοριακών Συστημάτων καθώς και όλα τα τερματικά.
- Όλο το προσωπικό (εσωτερικό και εξωτερικούς συνεργάτες) που εμπλέκεται στη διαχείριση και υποστήριξη συστημάτων.

3.10.4 Πολιτική

3.10.4.1 Αυτόματες Καταγραφές

Όλα τα ΠΕΣ πρέπει να τροποποιούνται κατάλληλα ώστε να συλλέγουν, με αυτοματοποιημένο τρόπο, κατ’ ελάχιστο τις ακόλουθες καταγραφές:

- Εκκίνηση και τερματισμός συστήματος.
- Αλλαγές διαμόρφωσης.
- Ενεργοποίηση και απενεργοποίηση υπηρεσιών.
- Εγκατάσταση και αφαίρεση λογισμικού.
- Ενημέρωση και τροποποίηση λογισμικού και υλισμικού.
- Ειδοποιήσεις και μηνύματα λάθους συστήματος.
- Σύνδεση και έξοδος χρηστών από το σύστημα.
- Προσβάσεις σε ευαίσθητες πληροφορίες και συστήματα.
- Δημιουργία, τροποποίηση ή διαγραφή λογαριασμού χρήστη.
- Τροποποίηση των δικαιωμάτων και των ελέγχων πρόσβασης.

Όλα τα τερματικά πρέπει να τροποποιούνται κατάλληλα ώστε να συλλέγουν, με αυτοματοποιημένο τρόπο, κατ' ελάχιστο τις ακόλουθες καταγραφές:

- Εκκίνηση και τερματισμός συστήματος.
- Σύνδεση και έξοδος χρηστών από το σύστημα.
- Ενεργοποίηση και απενεργοποίηση υπηρεσιών.
- Αλλαγές διαμόρφωσης.
- Εκτέλεση διεργασιών (installers, scripts).
- Σύνδεση συσκευών USB.
- Ειδοποιήσεις και μηνύματα λάθους συστήματος.

Όλα τα τερματικά πρέπει να ενσωματώνουν συστήματα Endpoint Detection and Response (EDR) και να παρέχουν καταγραφές για τις δραστηριότητες και τα ευρήματά τους.

Όλα τα δίκτυα πρέπει να ενσωματώνουν συστήματα Intrusion Detection System (IDS) και Intrusion Prevention System (IPS) και να παρέχουν καταγραφές για τις δραστηριότητες και τα ευρήματά τους.

Κάθε εγγραφή ελέγχου πρέπει να περιέχει κατ' ελάχιστο:

- Χρονοσφραγίδα (UTC timestamp + timezone).
- Κωδικός συμβάντος.
- Αναγνωριστικό χρήστη (αν υπάρχει).
- Αναγνωριστικό πηγής (π.χ. IP, hostname, process ID).
- Στοχευόμενος πόρος (π.χ. URL, file path, DB table, service).
- Ενέργεια (π.χ. read, write, delete, config-change, login).
- Αποτέλεσμα (επιτυχία, αποτυχία, κωδικοί λαθών).

Όλα τα συστήματα πρέπει να χρησιμοποιούν NTP και να συνδέονται σε ίδιας κατηγορίας και ασφαλές stratum για τον συγχρονισμό των εγγραφών.

Ευαίσθητες πληροφορίες, όπως οι κωδικοί πρόσβασης, δεν πρέπει να αποθηκεύονται στα αρχεία καταγραφής.

3.10.4.1 Χειροκίνητες Καταγραφές

Παράλληλα με τις αυτοματοποιημένες καταγραφές, πρέπει να τηρούνται και χειροκίνητες εγγραφές ελέγχου τόσο για σημαντικές εργασίες που επηρεάζουν τη δομή και λειτουργία των ΠΕΣ καθώς και για δραστηριότητες που δεν μπορούν να καταγραφούν με αυτοματοποιημένο τρόπο όπως π.χ. φυσικές παρεμβάσεις. Με αυτό τον τρόπο παρέχεται ολοκληρωμένη εικόνα για τις δραστηριότητες γύρω από ένα ΠΕΣ καθώς και πληροφορίες όπως η πρόθεση και τα επίπεδα έγκρισης κατά τη διερεύνηση περιστατικών.

Οι χειροκίνητες εγγραφές ελέγχου πρέπει να περιέχουν κατ' ελάχιστο:

- Χρονοσφραγίδα (UTC timestamp + timezone).

- Αναγνωριστικό αιτήματος (αν υπάρχει).
- Αιτών (αν υπάρχει).
- Έγκριση (αν απαιτείται).
- Εκτελεστής.
- Στοχευόμενο ΠΕΣ.
- Περιγραφή ενέργειας.
- Αποτέλεσμα (π.χ. επιτυχία, αποτυχία, rollback).

3.10.5 Έλεγχος

Οι αυτοματοποιημένες εγγραφές ελέγχου πρέπει να ελέγχονται περιοδικά από τους υπεύθυνους των ΠΕΣ για την επιβεβαίωση της ομαλής λήψης τους και τον έλεγχο της ορθής λειτουργίας των συστημάτων.

Για τα κρίσιμα συστήματα του Υπουργείου πρέπει να υλοποιείται αυτοματοποιημένη αποστολή των εγγραφών ελέγχου σε κεντρικό SIEM (π.χ. agent-based collection, rsyslog, cloud logs).

Οι υπεύθυνοι των ΠΕΣ καθορίζουν κατάλληλα όρια και συνθήκες για την ενεργοποίηση ειδοποιήσεων, έτσι ώστε να ανιχνεύονται έγκαιρα πιθανά περιστατικά κυβερνοασφάλειας. Ορίζουν επίσης το προσωπικό που θα διαχειρίζεται και θα συντονίζει τη διαδικασία απόκρισης σε περιστατικά κυβερνοασφάλειας. Εάν το έργο της διαχείρισης περιστατικών έχει ανατεθεί σε εξωτερικό ανάδοχο, ορίζεται το προσωπικό που θα έχει την επίβλεψης της διαδικασίας.

3.10.6 Αποθήκευση

Τα αρχεία εγγραφών ελέγχου θα διατηρούνται για τουλάχιστον δύο έτη. Πρέπει δε να αντιμετωπίζονται ως υλικό ύψιστης αξίας και να τηρούνται όλα τα μέτρα που προβλέπονται από τις πολιτικές αντιγράφων ασφάλειας και κρυπτογράφησης.

Μόνο εξουσιοδοτημένο προσωπικό πρέπει να έχει πρόσβαση στις εγγραφές ελέγχου και για την εκτέλεση συγκεκριμένων εργασιών επίβλεψης και ασφάλειας.

3.10.7 Αναθεώρηση

Η πολιτική αναθεωρείται τουλάχιστον ετησίως ή νωρίτερα σε περίπτωση αλλαγών στο τεχνολογικό ή κανονιστικό πλαίσιο καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας.

3.11 ΠΟΛΙΤΙΚΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ & ΑΝΑΚΤΗΣΗΣ (Backup & Restore Policy)

3.11.1 ΣΚΟΠΟΣ

Η παρούσα πολιτική καθορίζει το πλαίσιο για τη δημιουργία, αποθήκευση, διαχείριση και επαλήθευση αντιγράφων ασφαλείας (backup) των πληροφοριακών συστημάτων του Υπουργείου Πολιτισμού καθώς και για την ανάκτηση δεδομένων (restore) από τα εν λόγω αντίγραφα.

Το πλέον κρίσιμο στοιχείο ανθεκτικότητας είναι η δυνατότητα ταχείας και αξιόπιστης επαναφοράς δεδομένων και συστημάτων μετά από κυβερνοεπίθεση (π.χ. Ransomware) ή φυσική καταστροφή.

Στόχος είναι η διασφάλιση της διαθεσιμότητας, ακεραιότητας και συνέχειας των κρίσιμων δεδομένων.

3.11.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η πολιτική αυτή ισχύει για:

- Όλα τα πληροφοριακά συστήματα, βάσεις δεδομένων, εφαρμογές, συσκευές NAS/SAN, file servers, εικονικές και φυσικές υποδομές (on-premises ή cloud) του Υπουργείου.
- Όλους τους υπαλλήλους, διαχειριστές και συνεργάτες που εμπλέκονται στη διαχείριση, υποστήριξη ή ασφάλεια των συστημάτων.

3.11.3 Αρχές Πολιτικής

1. Περιοδικότητα. Τα backup εκτελούνται με καθορισμένη συχνότητα (καθημερινά, εβδομαδιαία, μηνιαία) ανάλογα με το επίπεδο κρισιμότητας του συστήματος.

2. RTO & RPO. Για κάθε κρίσιμο σύστημα ορίζεται Recovery Time Objective (RTO) και Recovery Point Objective (RPO), ώστε να καθορίζεται το αποδεκτό χρονικό όριο αποκατάστασης και η μέγιστη αποδεκτή απώλεια δεδομένων.

3. Κανόνας 3-2-1. Εφαρμόζεται η αρχή 3-2-1 Backup Rule – τρία αντίγραφα δεδομένων, σε δύο διαφορετικά μέσα αποθήκευσης, εκ των οποίων ένα βρίσκεται εκτός εγκατάστασης (off-site ή air-gapped).

4. Ασφάλεια & Κρυπτογράφηση. Όλα τα αντίγραφα ασφαλείας είναι κρυπτογραφημένα (AES-256), τόσο κατά την αποθήκευση (At Rest) όσο και κατά τη μεταφορά (In Transit), με ιδιαίτερη έμφαση στα προσωπικά ή ευαίσθητα δεδομένα (σύμφωνα με τον GDPR).
5. Δοκιμές Ανάκτησης (restore tests). Η εγκυρότητα κάθε backup επιβεβαιώνεται μέσω περιοδικών restore tests. Ένα αντίγραφο θεωρείται έγκυρο μόνο εφόσον έχει επαναφερθεί επιτυχώς.

6. Διαχείριση Μέσων & Καταστροφή. Ορίζεται ρητά ο χρόνος διατήρησης (retention period) ανά τύπο backup, καθώς και η διαδικασία ασφαλούς καταστροφής των μέσων/δεδομένων στο τέλος του κύκλου ζωής τους.

7. Περιορισμός Πρόσβασης. Η πρόσβαση επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

8. Τεκμηρίωση. Όλες οι ενέργειες καταγράφονται στο “Μητρώο Αντιγράφων Ασφαλείας”.

3.11.4 Διαδικασία Backup

- Πλήρες Backup (Full): Εκτελείται τουλάχιστον εβδομαδιαία.
- Αυξητικό Backup (Incremental): Εκτελείται καθημερινά.
- Ετήσιο Αρχείο (Archive): Δημιουργείται για λόγους συμμόρφωσης και ιστορικότητας.

Μέσα και τοποθεσίες:

- NAS/SAN με ενεργή κρυπτογράφηση at rest
- Off-site ή cloud backup σύμφωνα με τον κανόνα 3-2-1
- Air-gapped ή απομονωμένα μέσα για προστασία από ransomware

Διατήρηση:

- Ημερήσια (7 ημέρες)
- Εβδομαδιαία (1 μήνας)
- Μηνιαία (12 μήνες)
- Ετήσια (5 έτη)

3.11.5 Διαδικασία Ανάκτησης (Restore)

1. Η αίτηση ανάκτησης υποβάλλεται από τον προϊστάμενο υπηρεσίας ή υπεύθυνο συστήματος.
2. Η επαναφορά εκτελείται μόνο από εξουσιοδοτημένο διαχειριστή.
3. Ολοκληρώνεται εντός των καθορισμένων RTO/RPO.
4. Μετά την ανάκτηση ελέγχεται η ακεραιότητα και πληρότητα των δεδομένων.
5. Όλες οι ενέργειες καταγράφονται λεπτομερώς

3.11.6 Κρυπτογράφηση & Προστασία

Όλα τα αντίγραφα ασφαλείας πρέπει να είναι κρυπτογραφημένα τόσο κατά την αποθήκευση (at rest) όσο και κατά τη μεταφορά (in transit). Τα κλειδιά κρυπτογράφησης αποθηκεύονται σε ασφαλές σύστημα διαχείρισης (KMS/HSM) και δεν συνοδεύουν τα ίδια τα backup.

3.11.7 Διαχείριση Κρυπτογράφησης & Κλειδιών

Τα κλειδιά κρυπτογράφησης αποθηκεύονται σε ασφαλές KMS/HSM. Η πρόσβαση περιορίζεται αυστηρά και τα κλειδιά ανανεώνονται περιοδικά, με ασφαλή καταστροφή μετά τη λήξη ισχύος τους.

3.11.8 Ρόλοι & Ευθύνες

- Τμήμα Υποδομών και Δικτύων: Εκτέλεση, παρακολούθηση και τεκμηρίωση backup/restore.
- Υπεύθυνος Ασφάλειας Πληροφοριών: Εποπτεία συμμόρφωσης και αξιολόγηση κινδύνων.
- DPO: Διασφάλιση συμμόρφωσης με GDPR για τα αποθηκευμένα και ανακτημένα δεδομένα.
- Υπηρεσίες: Ενημέρωση για κρίσιμα δεδομένα και προτεραιότητες ανάκτησης (RTO/RPO).

3.11.9 Παρακολούθηση & Έλεγχος

- Καθημερινός έλεγχος επιτυχούς ολοκλήρωσης backup
- Μηνιαίες αναφορές κατάστασης
- Εξαμηνιαίες δοκιμές επαναφοράς (restore tests)
- Αξιολόγηση αποτυχιών ή αποκλίσεων από τους στόχους RTO/RPO

Τα ευρήματα καταγράφονται και επιδιορθώνονται άμεσα

3.11.10Αναθεώρηση

Η πολιτική αναθεωρείται ετησίως ή νωρίτερα, όταν απαιτείται, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

- Σε περίπτωση σημαντικών αλλαγών στην υποδομή
- Σε περίπτωση περιστατικών ασφάλειας
- Εφόσον προκύπτει ανάγκη για ενημέρωσή της για αλλαγές στην τεχνολογία

3.12 Πολιτική Φυσικής Ασφάλειας Πληροφοριακών Συστημάτων

3.12.1 Εισαγωγή

Η φυσική ασφάλεια αποτελεί θεμελιώδη παράμετρο της συνολικής ασφάλειας των πληροφοριακών συστημάτων του Υπουργείου. Σκοπός της είναι η εξασφάλιση ότι οι χώροι και ο εξοπλισμός που υποστηρίζουν κρίσιμα πληροφοριακά συστήματα προστατεύονται επαρκώς από φυσικές απειλές, ατυχήματα, περιβαλλοντικούς κινδύνους ή κακόβουλες ενέργειες.

3.12.2 Σκοπός

Η παρούσα πολιτική καθορίζει τις αρχές, τις απαιτήσεις και τις διαδικασίες που εφαρμόζονται για τη διασφάλιση της φυσικής προστασίας των πληροφοριακών πόρων του Υπουργείου, συμπεριλαμβανομένων εγκαταστάσεων, εξοπλισμού και υποδομών υποστήριξης (ρεύμα, ψύξη, επικοινωνίες). Δεν αφορά την προστασία του προσωπικού, των εγκαταστάσεων και της περιουσίας που δεν συνδέεται άμεσα με τις τεχνολογίες πληροφορικής.

Η εφαρμογή της πολιτικής αυτής αποσκοπεί:

- Στην πρόληψη μη εξουσιοδοτημένης φυσικής πρόσβασης, ζημιάς ή απώλειας.
- Στην προστασία της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριών.
- Στην ενίσχυση της επιχειρησιακής συνέχειας και της ασφάλειας του προσωπικού.

3.12.3 Πολιτική

3.12.3.1 Έλεγχος φυσικής πρόσβασης

- Η πρόσβαση σε χώρους που στεγάζουν πληροφοριακά συστήματα επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα ανάλογα με την κατηγοριοποίηση του πόρου και το επίπεδο κινδύνου.
- Οι χώροι αυτοί προστατεύονται μέσω μηχανισμών ελέγχου πρόσβασης (κάρτες, βιομετρικά μέσα, κωδικοί, φύλακες).
- Όλες οι είσοδοι και έξοδοι καταγράφονται και τηρούνται αρχεία πρόσβασης που περιλαμβάνουν κατ’ ελάχιστον: προσωπικό/επισκέπτες, χρονικό διάστημα, αιτιολογία.
- Επισκέπτες και προσωπικό χωρίς κατάλληλη διαβάθμιση ασφαλείας συνοδεύονται καθ’ όλη τη διάρκεια παραμονής τους από το εξουσιοδοτημένο προσωπικό.

3.12.3.2 Προστασία εγκαταστάσεων και περιβάλλοντος

Οι εγκαταστάσεις πρέπει να προστατεύονται από κινδύνους πυρκαγιάς, πλημμύρας, υγρασίας, υπερθέρμανσης, σκόνης και διακοπής ρεύματος.

- Οι χώροι φιλοξενίας κρίσιμων συστημάτων (Data Center, Server Room) πρέπει να διαθέτουν:
    - Σύστημα πυρανίχνευσης και καταστολής πυρκαγιάς.
    - Αδιάλειπτη παροχή ρεύματος (UPS) και ελεγχόμενο περιβάλλον.
    - Σύστημα παρακολούθησης θερμοκρασίας και υγρασίας.

- Τοποθέτηση του εξοπλισμού σε υπερυψωμένο πάτωμα.

- Τα συστήματα προστασίας πρέπει να υποβάλλονται κατ’ ελάχιστο σε ετήσιους ελέγχους λειτουργικότητας.

3.12.3.3 Προστασία εξοπλισμού και δεδομένων

- Ο εξοπλισμός πληροφορικής πρέπει να είναι τοποθετημένος σε ασφαλείς, ελεγχόμενους χώρους.
- Τα εφεδρικά μέσα αποθήκευσης δεδομένων φυλάσσονται σε διαφορετική (σε σχέση με τα πρωτότυπα), ασφαλή τοποθεσία.
- Πρέπει να λαμβάνονται μέτρα πρόληψης απώλειας ή κλοπής φορητών συσκευών και αποθηκευτικών μέσων.
- Η απομάκρυνση ή απόσυρση εξοπλισμού επιτρέπεται μόνο μετά από έγκριση και σύμφωνα με τις διαδικασίες ασφάλειας πληροφοριών.

3.12.4 Αναθεώρηση

Η πολιτική αναθεωρείται τουλάχιστον ετησίως ή νωρίτερα σε περίπτωση αλλαγών στο τεχνολογικό ή κανονιστικό πλαίσιο καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά φυσικής ή περιβαλλοντικής ασφάλειας.

3.13 ΠΟΛΙΤΙΚΗ ΑΠΟΔΕΚΤΗΣ ΧΡΗΣΗΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

3.13.1 Εισαγωγή

Η Πολιτική Αποδεκτής Χρήσης ρυθμίζει τα θέματα που αφορούν στη χρήση του Πληροφοριακού Συστήματος που υποστηρίζει τις δραστηριότητες του ΥΠ.ΠΟ. Η πολιτική αυτή συμβάλει στο να γνωρίζουν οι χρήστες ποιες ενέργειές τους θεωρούνται επιτρεπτές και ποιες μη επιτρεπτές.

Η αποτελεσματική ασφάλεια είναι μια συλλογική προσπάθεια που στηρίζεται στη συμμετοχή και την υποστήριξη του κάθε μέλους του προσωπικού που χειρίζεται πληροφορίες ή/και πληροφοριακά συστήματα.

3.13.2 Σκοπός

Σκοπός αυτής της πολιτικής είναι:

- Η αποτροπή πιθανών επιβλαβών συμβάντων που μπορεί να προκύψουν από κακή χρήση του ΠΕΣ του ΥΠ.ΠΟ.
- Η προστασία των χρηστών από τις συνέπειες που μπορεί να υποστούν από την εσφαλμένη χρήση του ΠΕΣ.
- Η διασφάλιση ότι οι χρήστες δεν θα καταχραστούν τις δυνατότητες χρήσης που τους παρέχονται προκειμένου να προβούν σε παράνομες ενέργειες.

3.13.3 Πεδίο Εφαρμογής

Η πολιτική αυτή απευθύνεται στα μέλη του προσωπικού του ΥΠ.ΠΟ. και στους συνεργάτες του ΥΠ.ΠΟ που χρησιμοποιούν και υποστηρίζουν δραστηριότητες του Υπουργείου.

Η Διεύθυνση Διαχείρισης Ανθρώπινου Δυναμικού στις ενέργειες πρόσληψης προσωπικού ή συνεργατών τους κοινοποιεί την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του ΥΠ.ΠΟ. και εξασφαλίζει με τη “Δήλωση Εργαζομένου” ότι έχουν λάβει γνώσει και αποδεχτεί την Πολιτική αυτή.

Η παρούσα θεματική πολιτική είναι υποχρεωτική και αποτελεί αναπόσπαστο μέρος της Πολιτικής Ασφάλειας.

3.13.4 Πολιτική

3.13.4.1 Γενική Χρήση και Ιδιοκτησία

1. Τα Πληροφοριακά Συστήματα συγκαταλέγονται στους πολυτιμότερους πόρους του ΥΠ.ΠΟ. και κάθε μέλος του προσωπικού έχει την υποχρέωση να τα χρησιμοποιεί με σύνεση.

2. Τα Πληροφοριακά Συστήματα που προσφέρονται στο προσωπικό του ΥΠ.ΠΟ αποτελούν περιουσιακό της στοιχείο και η χρήση τους πρέπει να γίνεται αποκλειστικά για τους σκοπούς του Υπουργείου.

3. Η χρήση των Πληροφοριακών Συστημάτων συνεπάγεται την ανάληψη ευθυνών και υποχρεώσεων που περιγράφονται στην Πολιτική Αποδεκτής Χρήσης.

3.14.4.2 Δικαιώματα και Υποχρεώσεις Χρηστών

Οι παρακάτω δραστηριότητες παρέχουν ένα πλαίσιο με τις επιτρεπόμενες και μη επιτρεπόμενες χρήσεις του Πληροφοριακού Συστήματος.

3.14.4.2.1 Χρήση συστημάτων και δικτύων

1. Το προσωπικό πρέπει να χρησιμοποιεί το ΠΕΣ του ΥΠ.ΠΟ. σύμφωνα με τα όσα προβλέπονται στην παρούσα Πολιτική Αποδεκτής Χρήσης.

2. Οι χρήστες οφείλουν να λαμβάνουν όλα τα μέτρα που υποδεικνύουν οι υπεύθυνοι του ΥΠ.ΠΟ. για τη διασφάλιση του απορρήτου των επικοινωνιών τους.

Το ΥΠ.ΠΟ. οφείλει να ενημερώνει τους χρήστες των παρεχόμενων υπηρεσιών τουλάχιστον κατά την σύναψη της μεταξύ τους σύβασης αλλά και σε τακτά χρονικά διαστήματα σχετικά με τα μέτρα που ενδείκνυται να λαμβάνουν για την προστασία του απορρήτου των επικοινωνιών τους , ιδίως σχετικά με κανόνες ορθής χρήσης των παρεχόμενων υπηρεσιών αλλά και τους τρόπους χρήσης τεχνολογιών και πόρων σχετικών με την ασφάλεια των πληροφοριών που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών.

4. Τα εφεδρικά αντίγραφα πρέπει να τυγχάνουν μεταχείρισης του ιδίου επιπέδου κρισιμότητας και ευαισθησίας με τα δεδομένα και τις εφαρμογές που αποθηκεύονται σ’ αυτά.

5. Τα εφεδρικά αντίγραφα πρέπει να μεταφέρονται σε μια ασφαλή, περιβαλλοντικά-ελεγχόμενη τοποθεσία εκτός του κτηρίου που φιλοξενεί το Μηχανογραφικό Κέντρο του ΥΠ.ΠΟ.

6. Κάθε σύστημα πρέπει να έχει ένα καθορισμένο πρόγραμμα διατήρησης εφεδρικών αντιγράφων που θα συμμορφώνεται με τις πολιτικές διατήρησης δεδομένων του ΥΠ.ΠΟ.

7. Περιοδικά πρέπει να εξετάζονται οι διαδικασίες λήψης εφεδρικών αντιγράφων και ανάκτησης δεδομένων από εφεδρικά αντίγραφα για να διασφαλιστεί ότι τα δεδομένα μπορούν να ανακτηθούν αποτελεσματικά από τα εφεδρικά αντίγραφα.

8. Το ΥΠ.ΠΟ. οφείλει να καταγράψει και να εφαρμόσει λεπτομερείς διαδικασίες για τη διεξαγωγή της λήψης εφεδρικών αντιγράφων, την ανάκτηση δεδομένων, την διεξαγωγή εξέτασης των εφεδρικών αντιγράφων, τη μεταφορά των ταινιών από/προς τις εγκαταστάσεις αποθήκευσης και την ανακύκλωση ή εξουδετέρωση των εφεδρικών αντιγράφων με τη πάροδο της περιόδου διατήρησής τους. Σκοπός των ενεργειών αυτών είναι η αποτροπή αποκάλυψης δεδομένων επικοινωνίας των χρηστών των παρεχόμενων υπηρεσιών σε μη εξουσιοδοτημένα άτομα.

9. Οι χρήστες οφείλουν να ενημερώνουν άμεσα τη Διεύθυνση Ηλεκτρονικής Διακυβέρνησης αν υποπέσει στην αντίληψή τους οποιοδήποτε κενό ασφάλειας συστήματος που θέτει σε κίνδυνο το απόρρητο επικοινωνιών των ίδιων ή άλλων χρηστών.

10. Οι χρήστες υποχρεούνται να συμμορφώνονται με την νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας.

11. Οι χρήστες δεν επιτρέπεται να συμμετέχουν σε οποιαδήποτε παράνομή δραστηριότητα, βάσει εθνικού ή ευρωπαϊκού δικαίου, κάνοντας χρήση των πληροφοριακών πόρων του ΥΠ.ΠΟ..

12. Δεν επιτρέπεται η χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο.

13. Δεν επιτρέπεται η χρήση οποιουδήποτε υλικού ή λογισμικού που δεν είναι σε γνώση της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης.

14. Η εγκατάσταση υλικού και λογισμικού στους Η/Υ των χρηστών γίνεται μόνο από το εξουσιοδοτημένο προσωπικό του Τμήματος Τεχνικής Υποστήριξης.

15. Οι χρήστες δεν πρέπει να παραβιάζουν τους ελέγχους πρόσβασης (access controls), ακόμα και αν αυτοί είναι ανεπαρκείς.

16. Δεν επιτρέπεται οποιαδήποτε ενέργεια μη εξουσιοδοτημένης χαρτογράφησης του δικτύου και η διεξαγωγή οποιασδήποτε μορφής παρακολούθησης του δικτύου του ΥΠ.ΠΟ.

17. Δεν επιτρέπεται η χρήση υπολογιστικών συστημάτων που δεν ανήκουν στο ΥΠ.ΠΟ. για εργασίες του ΥΠ.ΠΟ.

18. Τα μέλη του προσωπικού που διαθέτουν φορητό υπολογιστή, ο οποίος παρέχεται από το ΥΠ.ΠΟ. και χρησιμοποιείται για εργασιακούς σκοπούς, πρέπει να συμμορφώνονται με τις πολιτικές που ισχύουν για το σχετικό εξοπλισμό (Πολιτική Φορητών Υπολογιστών).

19. Δεν επιτρέπεται η εισαγωγή κακόβουλων προγραμμάτων στο δίκτυο ή τους κεντρικούς υπολογιστές (π.χ., ιοί, σκουλήκια, Δούρειοι Ίπποι, e-mail bombs, κ.λπ.).

20. Όλοι οι υπολογιστές που χρησιμοποιούνται από υπαλλήλους που συνδέονται με το Internet/Intranet/Extranet του ΥΠ.ΠΟ. πρέπει να εκτελούν συνεχώς το εγκεκριμένο λογισμικό ανίχνευσης ιών με μια ενημερωμένη βάση δεδομένων ιών.

21. Όλοι οι υπολογιστές πρέπει να κάνουν χρήση της λειτουργία προφύλαξης οθόνης (screensaver) με προστασία κωδικού πρόσβασης ή να γίνεται κλείδωμά του ηλεκτρονικού υπολογιστή κατά την απομάκρυνση του χρήστη.

22. Οι χρήστες υποχρεούνται να συμμορφώνονται με την εκάστοτε ισχύουσα “Πολιτική Κωδικών Πρόσβασης“ για τη σωστή επιλογή και διαχείριση αυτών.

3.14.4.2.2 Χρήση Ηλεκτρονικού Ταχυδρομείου και Παγκοσμίου Ιστού

1. Η πρόσβαση στο Διαδίκτυο παρέχεται στο προσωπικό του ΥΠ.ΠΟ. για να χρησιμοποιηθεί για τους σκοπούς του ΥΠ.ΠΟ. και για τη βελτίωση των γνώσεων και δεξιοτήτων του ανθρώπινου δυναμικού της.

2. Το ΥΠ.ΠΟ. διατηρεί το δικαίωμα να περιορίσει την πρόσβαση σε συγκεκριμένους Ισοτόπους (Web Sites) του Παγκόσμιου Ιστού (World Wide Web). Οι χρήστες που χρειάζονται πρόσβαση σε Ισοτόπους που η πρόσβαση έχει περιοριστεί έχουν το δικαίωμα να υποβάλλουν σχετικό αίτημα στο Τμήμα Υποδομών και Δικτύων της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης.

3. Οι χρήστες πρέπει να γνωρίζουν ότι οι δυνατότητες των γραμμών που συνδέουν το ΥΠ.ΠΟ. με το Διαδίκτυο είναι πεπερασμένες και κατά συνέπεια η κατάχρηση των υπηρεσιών του Διαδικτύου (πχ. η λήψη μμεγάλων αρχείων) περιορίζει τη χρήση του Διαδικτύου από τους συναδέλφους τους.

4. Οι χρήστες πρέπει να αποφεύγουν την επίσκεψη σε Ιστοσελίδες (Web Pages) με παράνομο λογισμικό ή άλλο πειρατικό οπτικοακουστικό υλικό. Οι χρήστες πρέπει να γνωρίζουν ότι η επίσκεψη αυτών των Ιστοσελίδων μπορεί να θέσει σε κίνδυνο την ασφάλεια του Πληροφοριακού Συστήματος.

3.14.5 Παρακολούθηση και έλεγχος εφαρμογής της πολιτικής

1. Τα δεδομένα που δημιουργούνται με τη χρήση του Πληροφοριακού Συστήματος του ΥΠ.ΠΟ αποτελούν ιδιοκτησία του ΥΠ.ΠΟ.

2. Για την διασφάλιση της καλής και ασφαλούς λειτουργίας των πόρων του Πληροφοριακού Συστήματος, η χρήση τους μπορεί να καταγράφεται από εξουσιοδοτημένα άτομα (π.χ. διαχειριστές συστημάτων και δικτύων). Η καταγραφή δεν αφορά το περιεχόμενο της ηλεκτρονικής μετάδοσης πληροφοριών.

3. Το ΥΠ.ΠΟ. διατηρεί το δικαίωμα να διενεργεί προγραμματισμένους ή έκτακτους ελέγχους για την τήρηση της Πολιτικής Αποδεκτής Χρήσης και για την τήρηση των πολιτικών που συμπεριλαμβάνονται στην ευρύτερη Πολιτική Ασφάλειας του ΥΠ.ΠΟ. Τους ελέγχους πραγματοποιούν εξουσιοδοτημένα για το σκοπό αυτό άτομα (Ελεγκτές Πληροφοριακών Συστημάτων) και τα μέλη του προσωπικού οφείλουν να συνεργαστούν μαζί τους. Το προσωπικό έχει δικαίωμα να ενημερωθεί για τα μέσα ελέγχου, τα κριτήρια ελέγχου και τα αποτελέσματα των ελέγχων που το αφορούν.

3.14.6 Αναθεώρηση και Αξιολόγηση

Η Διεύθυνση Ηλεκτρονικής Διακυβέρνησης φέρει την ευθύνη για την κατάρτιση κατάλληλης διαδικασίας, η οποία διασφαλίζει ότι η αναθεώρηση διεξάγεται όταν λαμβάνουν χώρα αλλαγές που επηρεάζουν τη βάση της αρχικής αποτίμησης του κινδύνου (π.χ. νέες αδυναμίες ή αλλαγές στην οργανωτική υποδομή).