

## ΚΑΝΟΝΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ – ΔΙΚΤΥΟΥ-Η/Υ Γ. Ν. ΣΑΜΟΥ

### Ρόλοι – Αρμοδιότητες Νοσοκομείου

Το Νοσοκομείο διαθέτει την ακόλουθη Πολιτική Ασφαλείας για την χρήση δεδομένων στην οποία περιγράφονται τα οργανωτικά και τεχνικά μέτρα που απαιτούνται ώστε να προστατεύονται τα πληροφοριακά συστήματα-δεδομένα και να αποφεύγεται η τυχαία απώλεια, η αθέμιτη χρήση, η αθέμιτη καταστροφή, η απαγορευμένη διάδοση, η παράτυπη πρόσβαση και κάθε μορφή χρήσης που αντίκειται στο νόμο, τις αρχές δεοντολογίας και ηθικής.

- Καθήκον του νοσοκομείου είναι να λαμβάνει όλα εκείνα τα μέτρα για να εξασφαλίζει ότι η Πολιτική Ασφαλείας τηρείται και ότι δεν παραβιάζεται.
- Ευθύνη του Νοσοκομείου είναι να εξασφαλίζει την ασφάλεια των δεδομένων και των πληροφοριακών συστημάτων, την ακεραιότητα του εξοπλισμού και των υπολογιστών.
- Το Νοσοκομείο θα επιφυλάσσεται για κάθε νόμιμο δικαίωμα του σε κάθε περίπτωση απώλειας ή ζημιάς σε προσωπικά δεδομένα εφόσον αυτό προκύπτει αποδεδειγμένα από αμέλεια του χρήστη.
- Το Νοσοκομείο προσπαθεί να προστατεύσει την όποια απώλεια πληροφοριών. Αν απώλεια πληροφορίας στο σύστημα οφείλεται σε αμέλεια εκ μέρους του προσωπικού ή σε οποιαδήποτε αποτυχία του υλικού ή του λογισμικού που είναι πέρα από τα όρια του χρήστη, το Νοσοκομείο θα προσπαθήσει να αποκαταστήσει την απώλεια αυτή και τα δεδομένα αυτά.
- Οι εγκαταστάσεις σε συστήματα, υπολογιστές και δίκτυα ανήκουν στο Νοσοκομείο και χρησιμοποιούνται υπέρ της αποστολής του. Είναι δικαίωμα του Νοσοκομείου να περιορίσει ή να επεκτείνει την πρόσβαση στις υπηρεσίες αυτές.
- Οι παραπάνω εγκαταστάσεις δεν μπορούν να χρησιμοποιηθούν για οποιαδήποτε εμπορική δραστηριότητα.
- Στόχος του Νοσοκομείου είναι να προστατεύει την εμπιστευτικότητα των πληροφοριών και να καθοδηγεί το προσωπικό του ώστε και αυτό να κάνει το ίδιο.
- Το Νοσοκομείο διατηρεί το δικαίωμα να περιορίσει προσωρινά ή μόνιμα τη χρήση των υπολογιστικών συστημάτων σε όποιον χρήστη αποδειχτεί ότι σκοπίμως προσπάθησε να αντιγράψει, αφαιρέσει ή να αλλάξει όποιες πληροφορίες χωρίς έγγραφη άδεια.
- Στην προσπάθεια του αυτή το Νοσοκομείο διατηρεί το δικαίωμα να λάβει και άλλα μέτρα προκειμένου να προστατεύσει την ακεραιότητα εξοπλισμού, δεδομένων από κάθε αναρμόδια ή χρήση (όπως λήξη-τερματισμό ενός προγράμματος ή μιας σύνδεσης στο Internet), ή την προσωρινή αλλαγή ονομάτων και κωδικών πρόσβασης ενός χρήστη στα συστήματα του.
- Το Νοσοκομείο μέσω των Διαχειριστών Συστημάτων ή άλλων εξουσιοδοτημένων ατόμων διατηρεί το δικαίωμα να ελέγχει περιοδικά τις εγκαταστάσεις του, τα Πληροφοριακά Συστήματα τους Υπολογιστές και την πληροφορία που διακινείται στο δίκτυο του.
- Πληροφοριακές Υποδομές/ Σύστημα λογίζεται το σύνολο των υποδομών πληροφορικής όπως Η/Υ, Εκτυπωτές, περιφερειακά, λογισμικά, ενεργά στοιχεία δικτύου και καλώδια υποδομών LAN.

- Αρμόδια για την μεταβολή και αναθεώρηση του παρόντος κανονισμού είναι μόνο το Δ.Σ. του νοσοκομείου κατόπιν εισηγήσεως του (αρμόδιου τμήματος) .

Σκοπός του παρόντος κανονισμού είναι να ενημερώσει και να περιγράψει με σαφήνεια, τους όρους λειτουργίας και τους κανόνες πρόσβασης των χρηστών στο Δίκτυο και στα Υπολογιστικά Δεδομένα του Γ. Ν. Σάμου.

### **Κανόνες Χρηστών**

- Τα δεδομένα που διαχειρίζονται τα πληροφοριακά συστήματα του Νοσοκομείου είναι, κατά κύριο λόγο, ευαίσθητα δεδομένα προσωπικού χαρακτήρα. Τα δεδομένα αυτά είναι απόρρητα και η επεξεργασία τους επιτρέπεται κατ' εξαίρεση σύμφωνα με το Νόμο 4624/2019. Υπό αυτό το νομικό πλαίσιο, οι χρήστες υποχρεώνονται να προστατεύουν το απόρρητο των ιατρικών πληροφοριών που συλλέγουν και επεξεργάζονται και να διατηρούν την ακεραιότητα των δεδομένων, φροντίζοντας ώστε τα ιατρικά δεδομένα να είναι ακριβή. Απαγορεύεται η εξαγωγή και η διαβίβαση ευαίσθητων προσωπικών δεδομένων από τους χρήστες χωρίς την προηγούμενη άδεια του Νοσοκομείου.
- Τα πληροφοριακά συστήματα (ή οι ηλεκτρονικές πληροφορίες) μπορούν να χρησιμοποιηθούν μόνο από τους εργαζόμενους στο νοσοκομείο. Όποια άλλα πρόσωπα τα χρησιμοποιήσουν χρειάζονται έγγραφη άδεια από Δ.Σ. του Νοσοκομείου. Η άδεια αυτή μπορεί να εκχωρηθεί από τους διαχειριστές συστήματος εφόσον πρόκειται για συνεργαζόμενες εταιρίες που συντηρών πληροφοριακές υποδομές (π.χ. Siemens για τον αξονικό, Πληροφορικής Ελλάδος για τα μικροβιολογικό Abbot αιμοδοσία κλπ).
- Οι εργαζόμενοι του νοσοκομείου έχουν προσωπική ευθύνη να γνωρίζουν, να τηρούν και να συμμορφώνονται με την πολιτική ασφαλείας όπως αυτή διαμορφώνεται, ανανεώνεται συνεχώς από το Τμήμα Πληροφορικής.
- Όλοι οι χρήστες που χρησιμοποιούν τα πληροφοριακά συστήματα είναι υπεύθυνοι για τη σωστή χρήση τους. Καθήκον τους είναι να εκτελούν κάθε έλεγχο στην προσπάθεια να αποτρέψουν κακή χρήση των πληροφοριακών συστημάτων και να προστατεύουν δεδομένα. Ο χρήστης είναι υπεύθυνος για τις πράξεις του στα προγράμματα, στον εξοπλισμό, στις συνδέσεις του και για προστασία των δεδομένων που διαχειρίζεται.
- Κανένα χρήστης από οποιαδήποτε σκόπιμη πράξη δεν μπορεί να διακινδυνεύσει την ακεραιότητα του εξοπλισμού, των λειτουργικών συστημάτων, των προγραμμάτων ή άλλων αποθηκευμένων πληροφοριών είτε μέσα στο νοσοκομείο είτε όπου αλλού αποκτά πρόσβαση μέσω δικτύου.
- Ο χρήστης πρέπει να χειρίζεται τα προγράμματα σύμφωνα με τις οδηγίες χρήσης .Να σέβεται το copyright, τις άδειες χρήσης και τα πνευματικά δικαιώματα των κατασκευαστών. Κανένας δεν μπορεί να χρησιμοποιήσει, να αντιγράψει ή να μεταφέρει οποιαδήποτε λογισμικό του νοσοκομείου εκτός του οργανισμού εάν δεν υπάρχει έγγραφη άδεια από τον κατασκευαστή του λογισμικού.
- Ο χρήστης αποδέχεται ότι η χρήση των πληροφοριακών υποδομών είναι τίμια και νόμιμη και να λαμβάνει υπόψη τα δικαιώματα, τις ιδιαιτερότητες και τις ευαισθησίες των άλλων ανθρώπων.
- Ο χρήστης υποχρεούται να κάνει σωστή χρήση του ηλεκτρονικού ταχυδρομείου και των υπηρεσιών του δικτύου (INTERNET). Να μην στέλνει

ηλεκτρονικά μηνύματα εξ' ονόματι άλλων χρηστών ή να προωθεί διαφημιστικά μηνύματα ηλεκτρονικού ταχυδρομείου.

- Ο χρήστης απαγορεύεται να προωθεί ηλεκτρονική αλληλογραφία που αφορά υποθέσεις του νοσοκομείου, σε οποιονδήποτε τρίτο που δεν εμπλέκεται σε αυτές χωρίς έγγραφη άδεια του νοσοκομείου.
- Ο χρήστης επιτρέπεται να κάνει χρήση του διαδικτύου σε λογικά πλαίσια και να μην οδηγείται σε πράξεις που δημιουργούν υψηλή κυκλοφορία άσκοπων δεδομένων μέσα στο δίκτυο και ενέργειες που μειώνουν την απόδοση του δικτύου και δυσκολεύουν την εργασία του άλλου προσωπικού. Αρμόδιος να κρίνει «τα λογικά πλαίσια» είναι ο διαχειριστής των πληροφοριακών συστημάτων.
- Το όνομα χρήστη και ο κωδικός πρόσβασης στα πληροφοριακά συστήματα πρέπει να χρησιμοποιούνται μόνο από τον κάτοχο του κωδικού. Ο κωδικός είναι αυστηρά ιδιωτικός και δεν διανέμεται σε άλλο χρήστη εκτός από εξαιρετικές περιπτώσεις (Με συμφωνία του Τμήματος Πληροφορικής ή του προϊσταμένου/νου του/της). Ο κωδικός χορηγείται μετά από σχετικό υπογεγραμμένο αίτημα του χρήστη στο Τμήμα Πληροφορικής.
- Σε κανέναν χρήστη δεν επιτρέπεται η πρόσβαση ή τροποποίηση στο υλικό των υπολογιστών. Αυτό είναι ευθύνη μόνο του Τμήματος Πληροφορικής. Με τον όρο υλικό εννοούνται υπολογιστές, εκτυπωτές, διασυνδεδεμένα περιφερειακά, ενεργά στοιχεία και καλωδίωσης δικτύου.
- Ο χρήστης πρέπει να παίρνει τις απαραίτητες προφυλάξεις για να διασφαλίζει τα δεδομένα και τον εξοπλισμό κάνοντας καλή (σωστή) χρήση των παραπάνω.
- Οι παραβιάσεις των παραπάνω κανόνων θα ελέγχονται και αν απαιτείτε θα αμφισβητείται η πρόσβασή του σε όλες τις εγκαταστάσεις των υπολογιστών του νοσοκομείου κατόπιν εισήγησης του Τμήματος Πληροφορικής στη Διοίκηση του Νοσοκομείου.

### **Οδηγίες – Κατευθυντήριες γραμμές για τους χρήστες**

- Να προστατεύουν και να μην αποκαλύπτουν δεδομένα, προσωπικές πληροφορίες, εμπιστευτικά στοιχεία στα οποία έχουν πρόσβαση. Απαγορεύεται η εξαγωγή και η διαβίβαση ευαίσθητων προσωπικών δεδομένων από τους χρήστες χωρίς την προηγούμενη άδεια του Νοσοκομείου.
- Να κρατούν αυστηρά ιδιωτικό τον κωδικό πρόσβασης και να μην τον μοιράζονται με οποιονδήποτε άλλο.
- Να αλλάζουν περιοδικά τους κωδικούς πρόσβασης.
- Να σέβονται τους προσωπικούς κωδικούς των άλλων.
- Να μην κάνουν παράνομα αντίγραφα προγραμμάτων
- Να μην αλλάζουν σκόπιμα τμήματα του λογισμικού ή των προγραμμάτων χωρίς την ενημέρωση όλων των εμπλεκόμενων σε αυτά.
- Να μην κατέχουν εσκεμμένα, να μην δίνουν σε άλλο πρόσωπο, να μην εγκαθιστούν ή να τρέχουν προγράμματα που δημιουργούν προβλήματα στη χρήση υπολογιστών και συστημάτων. Τα προγράμματα αυτά συνήθως είναι ιοί (viruses: Trojan horses, worms, password breakers, packet observers, torrent clients, Tor Browsers, P2P clients Κλπ).
- Να μην συνδέουν οποιαδήποτε ηλεκτρονική συσκευή στις εγκαταστάσεις Η/Υ και δικτύων με σκοπό τον έλεγχο στοιχείων, πακέτων, σημάτων ή άλλων πληροφοριών.

- Να σέβονται το copyright, τις άδειες χρήσης και τα πνευματικά δικαιώματα όπου υπάρχουν.
- Να μην χρησιμοποιούν τον υπολογιστή για να ενοχλήσουν, παρενοχλήσουν, τρομοκρατήσουν, εκφοβίσουν, απειλήσουν, προσβάλλουν με οποιοδήποτε τρόπο άλλο χρήστη μέσα ή έξω από το νοσοκομείο.
- Οι εγκαταστάσεις του Νοσοκομείου δεν μπορούν να χρησιμοποιηθούν για μετάδοση, λήψη επίδειξη κάθε λογής διαφήμισης ή απαράδεκτου υλικού (π.χ. παιδική πορνογραφία, άρθρα που υποκινούν το έγκλημα ή τη βία, όποιας μορφής παρενόχληση κ.λπ.) .
- Να μην κάνουν σκόπιμη σπατάλη του δικτύου.
- Ευθύνη των χρηστών είναι η ασφάλεια και η ακεραιότητα των δεδομένων που αποθηκεύονται στο προσωπικό υπολογιστικό σύστημα που κατέχουν. Όπως επίσης και η αποθήκευση (αντίγραφα ασφαλείας, backup) των αρχείων τους σε usb, cd ή άλλα μέσα. Σε περίπτωση που τα δεδομένα αυτά είναι κρίσιμα για την υπηρεσία θα πρέπει να το αναφέρουν στο Τμήμα Πληροφορικής για σχετικές ενέργειες. Σε καμία περίπτωση το Τμήμα Πληροφορικής δεν είναι υπεύθυνο για την απώλεια των δεδομένων που αποθηκεύονται «τοπικά» στον Η/Υ του κάθε χρήστη και για λόγους GDPR. Ο χρήστης θα πρέπει να αποθηκεύει τα προσωπικά του αρχεία περιοδικά σε εξωτερικό μέσο αποθήκευσης usb κτλ .
- Η αποθήκευση αρχείων προσωπικού χαρακτήρα στους Η/Υ του Νοσοκομείου αποτελεί αυστηρά ευθύνη του κάθε χρήστη ως προς την ασφάλη, την σωστή, την εύρυθμη λειτουργία, και τη μετάδοση ιόν.
- Αποφεύγουμε όσο το δυνατό την μεταφορά αρχείων μέσω usb επιλέγουμε το ηλεκτρονικό ταχυδρομείο (το usb θα πρέπει να χρησιμοποιείτε πρωτίστως για τη διαδικασία back up).
- Η τηλεργασία που πρόσφατα καθιερώθηκε στο δημόσιο θα πρέπει να ενεργοποιείτε κατόπιν σχετικού αιτήματος του χρήστη καθώς και την έγκριση της Διοίκησης και εφόσον ολοκληρωθούν οι απαραίτητες διαδικασίες από το τμήμα Πληροφορικής.
- Η χορήγηση Υλικού Πληροφορικής γίνεται μετά από σχετικό αίτημα προς το Τμήμα Πληροφορικής και αν πρόκειται για νέο υλικό απαιτείται η έγκριση της Διοίκησης.
- Να μην παραπιεί τις ετικέτες χαρακτηρισμού εξοπλισμού (αριθμός μητρώου barcode παγίου εφόσον υπάρχει).

### **Κατάλληλη Χρήση του ηλεκτρονικού ταχυδρομείου**

- Να μην χρησιμοποιούν το E-MAIL για λόγους που θα φοβίσουν ή θα παρενοχλήσουν άλλους χρήστες
- Να μην στέλνουν μηνύματα που μπορεί να παρεμποδίσουν την αποδοτικότητα του συστήματος
- Να μην διαβάζουν το E-MAIL άλλου χρήστη χωρίς την άδεια του
- Να μην στέλνουν μηνύματα που είναι επιβλαβή για το Νοσοκομείο ή συγκρούονται με τα συμφέροντα του Νοσοκομείου

- Να μην απαντούν ή διαβάζουν μηνύματα που ο αποστολέας είναι άγνωστος ή ύποπτος για το σύστημα
- Να μην στέλνουν μηνύματα που περιέχουν άσεμνο, δυσάρεστο ή δυσφημιστικό υλικό.
- Η υποκλοπή μηνυμάτων μπορεί να συμβεί συχνά. Να είναι οι χρήστες προσεκτικοί όταν στέλνουν ιδιωτικές ή άλλες πληροφορίες (π.χ. να μην στέλνουν μηνύματα με προσωπικούς κωδικούς, κωδικούς πρόσβασης, κωδικούς πιστωτικών καρτών)
- Τα έγγραφα που περιέχουν ευαίσθητα προσωπικά δεδομένα πρέπει να κρυπτογραφούνται προτού αποσταλούν μέσω email.

## Όροι και Οδηγίες Διαδικτύου

- Η σύνδεση στο διαδίκτυο γίνεται μόνο από το Τμήμα Πληροφορικής μετά από αίτηση του προϊσταμένου του χρήστη.
- Να μην επισκέπτονται οι χρήστες σελίδες που δεν είναι σίγουρο ότι είναι ασφαλείς για το δίκτυο ή για τον προσωπικό υπολογιστή τους.
- Να μην «κατεβάζουν», μεταφέρουν (download) ή αντιγράφουν λογισμικό χωρίς προηγούμενη άδεια του προμηθευτή ή κατασκευαστή του λογισμικού.
- Ότι λογισμικό κατεβαίνει από το διαδίκτυο πρέπει να ελεγχθεί από ιούς. Αν δεν εμπιστευόμαστε τον παροχέα του λογισμικού, το υλικό πρέπει να τεσταριστεί σε ένα Standalone Non-Production Μηχάνημα (Αυτόνομο Μηχάνημα Μη Παραγωγικό). Αν το Software περιέχει ιό, τότε η ζημιά θα περιοριστεί μόνο στο μηχάνημα αυτό.
- Δεν υπάρχει καμία διαδικασία ποιοτικού ελέγχου στο διαδίκτυο και μια σημαντική ποσότητα πληροφορίας είναι ξεπερασμένη ή ανακριβής. Οι χρήστες να είναι πάντα προσεκτικοί στις πληροφορίες που στέλνονται μέσω διαδικτύου.
- Να αποφεύγεται να κατεβαίνει λογισμικό που μπορεί να προκαλέσει αναταραχή στο δίκτυο ή να καταναλώνει σημαντικό μέρος της απόδοσης του.
- Οι χρήστες να μην συμμετέχουν σε Multi-User Internet Applications (πολλών χρηστών εφαρμογές δικτύου), χωρίς εξουσιοδότηση ή έγγραφη άδεια.
- Να μην χρησιμοποιούν την σύνδεση με το δίκτυο για να καθιερώσουν (establish) νέα κανάλια ανώνυμης ηλεκτρονικής επικοινωνίας που περιλαμβάνουν ηλεκτρονική ανταλλαγής δεδομένων όπως (tor, P2P, Torrents).
- Οι χρήστες να είναι πάντα προσεκτικοί στις πληροφορίες που στέλνονται μέσω διαδικτύου. Πρέπει να επιλέγουν κρυπτογραφημένα κανάλια μετάδοσης https και να αποφεύγουν τα μη κρυπτογραφημένα http. Διαφεύγει της αρμοδιότητας των διαχειριστών να εγγυηθούν για την ακεραιότητα των δεδομένων εφόσον το ένα άκρο δεν είναι εντός του νοσοκομείου.
- Το Νοσοκομείο «ενθαρρύνει» το προσωπικό να χρησιμοποιεί το διαδίκτυο (επισκεπτόμενο ομάδες ειδήσεων ή άλλες δραστηριότητες), αλλά αν η εξερεύνηση είναι για προσωπικούς λόγους αυτή θα πρέπει να γίνεται σε μη εργάσιμη ώρα.
- Χρήστης που θέλει να συνδέσει το Laptop σε θέση δικτύου πρέπει να παίρνει άδεια από το Τμήμα Πληροφορικής.
- Οι προσωπικές συσκευές tablet, Smart Phone κλπ πρέπει να συνδέονται αυστηρά μόνο στο ασύρματο δίκτυο των επισκεπτών το οποίο δεν συσχετίζεται με το δίκτυο των πληροφοριακών συστημάτων του νοσοκομείου.

## Γενικές Πληροφορίες

Οποιασδήποτε αλλαγές στα συστήματα, στο λογισμικό, στα προγράμματα εφαρμογών πρέπει:

- Να είναι εξουσιοδοτημένες και εγκεκριμένες από την υπηρεσία
- Να είναι λεπτομερώς δοκιμασμένες
- Να είναι τεκμηριωμένες, σαφείς και αποτελεσματική για την υπηρεσία
- Να είναι εφαρμόσιμες
- Να εγκατασταθεί από κατάλληλο εξουσιοδοτημένο προσωπικό ή το Τμήμα Πληροφορικής

Υπεύθυνοι και επιβλέποντες των αλλαγών είναι το Τμήμα Πληροφορικής και ο/η προϊστάμενος/νη αρχή του τμήματος που γίνεται η αλλαγή.

## Διαχειριστές Συστήματος

- Έχουν την ευθύνη να διατηρούν την ακεραιότητα των Πληροφοριακών Συστημάτων και Δεδομένων και να σιγουρεύονται ότι δεν θα αλλοιωθούν ή καταστραφούν εύκολα.
- Έχουν επιπλέον προνόμια πρόσβασης στην προσπάθεια να ανταποκριθούν στις δραστηριότητες τους.
- Έχουν καθήκον να χρησιμοποιούν αυτά τα προνόμια σαν επαγγελματίες και μέσα στα πλαίσια της εργασίας τους.
- Να σιγουρεύονται ότι οι χρήστες εκτελούν τα δικά τους καθήκοντα με σεβασμό στη σύνδεση τους στα συστήματα και στο δίκτυο.
- Να παρέχουν στους χρήστες ακριβείς πληροφορίες και συμβουλές για τη χρήση των προγραμμάτων, να παρέχουν και να λαμβάνουν πληροφορίες για λύσεις σε τυχόν προβλήματα.
- Να προσπαθούν για την σωστή χρήση των Πληροφοριακών Συστημάτων και να εισηγούνται για τη προμήθεια των κατάλληλων εργαλείων ασφαλείας.
- Διατηρούν το δικαίωμα για έκτακτες πράξεις με σκοπό να εξασφαλίσουν τα παραπάνω. Οι πράξεις αυτές περιλαμβάνουν τερματισμό προγραμμάτων, κλείσιμο server, προσωρινή αλλαγή ή απενεργοποίηση κωδικών και αποσύνδεση συσκευών στο δίκτυο.

## Πρέπει να ειδοποιούνται άμεσα όταν:

1. Ευαίσθητα δεδομένα χάνονται, αποκαλύπτονται σε αναρμόδια μέρη ή όταν οι χρήστες υποψιάζονται απώλεια ή αποκάλυψη τέτοιων πληροφοριών
2. Οι κωδικοί πρόσβασης χάνονται, κλέβονται ή αποκαλύπτονται, ή οι χρήστες υποψιάζονται απώλεια, κλοπή ή αποκάλυψη κωδικών.
3. Ένας χρήστης αλλάζει τμήμα ή συνταξιοδοτείται.
4. Υπάρχει ασυνήθιστη συμπεριφορά του συστήματος (όπως να λείπουν αρχεία, να γίνονται συχνά συντριβές συστημάτων-System crashes, να εμφανίζονται πολλαπλά μη εξουσιοδοτημένα παράθυρα Pop Up κατά την περιήγηση τους στο διαδίκτυο)