



## נספח ד'

### הנחיות אבטחת מידע והגנת הפרטיות לספק שירות

#### ניהול שינויים

שינוי	גרסא	מחבר	תאריך
גיבוש מסמך הנחיות אבטחת מידע והגנת הפרטיות לספק שירות	1.0	רענן עייש	14/11/2019
עדכון מסמך הנחיות אבטחת מידע והגנת הפרטיות לספק שירות	1.1	רענן עייש	19/05/2021

הספק מצהיר ומתחייב כי בביצוע התחייבויותיו בהסכם זה, יעמוד בכל דרישות אבטחת המידע של המזמינה, כמפורט ב נספח הנחיות אבטחת מידע והגנת הפרטיות לספק שירות.

#### היבטי אבטחת מידע

1. הספק מצהיר ומתחייב, כי ינקוט בכל אמצעי אבטחת המידע הנדרשים לצורך הבטחת שלמות המידע של המזמין, זמינותו, סודיותו, שרידותו ואמינותו, ובכלל זאת אמצעים למניעת גישה של גורמים בלתי מורשים למידע (בין אם גורמים מטעמו של הספק ו/או כל צד שלישי אחר) ולמניעת זליגתו - בין אם מדובר במידע של המזמין המאוחסן ו/או מעובד במערכות המידע של הספק ובין אם בעת העברת המידע מהמזמין לספק ו/או מהספק למזמין.

הספק יפעל באופן שוטף לצמצום החשיפה לאיומי סייבר בחצרותיו ובכלל זאת ינקוט בפעולות הבאות: הקשחת מערכות ותשתיות; פיתוח מאובטח; צמצום הרשאות של משתמשים על פי העקרונות של הצורך לדעת (Need to Know) והרשאות מינימליות (Least Privileged); בקרה וחסויה של התקנים ניידים; סינון סוגי קבצים נכנסים למערכות הספק; סינון הודעות דוא"ל ממענים לא מוכרים או חשודים; חסימת מתחמי כתובות ו/או סוגי רשתות המשמשות כמקור להתקפות; הצפנת המידע.

2. הספק מתחייב כי מערכות המחשבים והמידע המשמשות אותו מוגנות מפני גישה ו/או חדירה בלתי מורשית למידע וכי כל תחנות הקצה, השרתים וכל מערכת מידע אחרת מוגנים באמצעים טכנולוגיים המגנים מפני נגיפי מחשב, רוגלות, כפרות וכל תוכנה ואמצעי זדוני אחר והמבטיחים רמת אבטחת מידע גבוהה.

3. הספק מתחייב לפעול לפי הוראות כל דין (לרבות כל הנחיה של רשות מוסמכת) ולנקוט על חשבונו בכל הצעדים הסבירים הדרושים לאבטחת המידע ומערכות המידע המשמשות אותו. המזמין יעדכן את אמצעי



האבטחה באופן שוטף על-פי המתחייב מההתפתחויות הטכנולוגיות, התקנים, הנהלים והסטנדרטים התעשייתיים בתחום אבטחת מידע.

4. באחריות הספק להדריך את עובדיו ו/או מי שעוסק מטעמו באספקת השירותים, ובפרט כל מי שהוא בעל גישה למידע של המזמין, לגבי הוראות ההסכם ויישומן, בכדי לוודא שעקרונות אבטחת המידע יישמרו לאורך כל תקופת ההסכם וככל הנדרש אף לאחר סיומו. הספק יפתח תכנית הדרכה לעובדיו, לפיה העובד ילמד מהו השימוש המותר והאסור במערכות התפעוליות והעסקיות של הספק ובאילו מקרים עליו לדווח לצוותים הממונים על תקרית חשודה במערכות הספק.

הספק ממנה מטעמו את (לציין את שמו ופרטיו של הנציג) \_\_\_\_\_ לאיש הקשר מטעמו לצורך כך. איש הקשר יפעל מול נציג המזמין לצורך יישום כל הוראות ההסכם, לרבות טיפול ביישום דרישות אבטחת המידע וליישום מנגנוני ההטמעה וההדרכה של הוראות ההסכם שעניינן באבטחת מידע. הספק מתחייב כי כל עובדיו ו/או מי מטעמו החשוף למידע לא יעסוק באספקת השירותים למזמין ולא תתאפשר לו הרשאת גישה למידע, מבלי שקיבל הדרכה כאמור. ביצוע ההדרכות יתועד בכתב (לרבות תאריכים) לצורך הוכחת קיומן.

5. מבלי לגרוע מכל הוראה אחרת בהסכם זה, ובפרט זה סעיף הסודיות, ידוע לספק והוא מאשר כי חל עליו איסור חמור להעביר את המידע לכל צד שלישי או להשתמש בו לכל שימוש אחר השונה מהמטרות שהוגדרו בהסכם זה, בלא אישור בכתב ומראש מהמזמין.

6. הספק לא יתיר גישה למידע, אלא לבעלי התפקידים אצל הספק שהדבר חיוני לעבודתם במסגרת אספקת השירותים למזמין על-פי הסכם זה;

7. המערכת תותאם באופן מלא לעבודה על מערכת הפעלה חלונות 10 ותשודרג במסגרת תקופת ההתקשרות לעבודה בפלטפורמות חדשות של מערכת הפעלה חלונות.

8. הספק מתחייב לדווח למנהל אבטחת המידע של מרכז רפואי ברזילי לאלתר, על כל פגיעה או חשד לפגיעה בסודיות המידע ו/או על זליגתו לצד שלישי כלשהו לאיש הקשר שמינה המזמין. בכלל זה, הספק יקבע נוהל לתגובה, לדיווח ולניהול תקריות אבטחה הקשורים, או שקיים חשד שהם קשורים במידע של המזמין. הספק יקיים רישום לכל תקרית אבטחה שהגיעה לידיעתו, ובו יתועד מועד התקרית, זהות המדווח, זהות הנמענים של הדיווח ותוצאות התקרית. דיווח על תקרית אבטחה יימסר למזמין בהקדם האפשרי, ביחד עם מלוא הפרטים הרלבנטיים לאירוע. המזמין רשאי לדרוש שהספק יוסיף פרטים ו/או יוסיף ויעדכן אותה ביחס להתפתחות האירוע או חקירתו, והספק מתחייב לפעול לפי דרישת המזמין.

9. בכל מקרה בו הספק יוציא מרשותו ו/או מחזקתו ו/או ממרכז רפואי ברזילי, מחשבים או כל ציוד אחר, לרבות אלו שבשימוש מערכות המידע והנדסה רפואית אותן הוא סיפק, לצורך תיקון או החזוקה במיקור חוזן, או לצורך החלפה או גריטה, הרי שהוא מתחייב למחוק את כל המידע שהגיע אליו והשמור במדיה המגנטית וברכיבי הזיכרון האוגרים אותו, באופן שלא יהיה ניתן לשחזרו.



10. העברת המידע בין הספק לבין המזמין תיעשה באחד מהאמצעים הבאים בלבד -

10.1. העברת מידע רפואי ממוכנת ע"י תשתית כספות/ MFT

10.2. העברת מידע ממוחשבת, תוך הצפנת תווך התקשורת קצה לקצה למניעת שינוי המידע ו/או גישה בלתי מורשית אליו;

10.3. העברת מדיה מגנטית באמצעות שליח המאושר ע"י המזמין, כאשר העברת המידע תיעשה ללא עצירות ביניים וקבלת אישור מסירה של הספק.

המזמין יהיה רשאי לדרוש מעת לעת לשנות את אופן העברת המידע בהתאם לצרכים ולהתפתחויות הטכנולוגיות, לפי שיקול דעתו הבלעדי.

11. הספק ישתף פעולה בתום-לב, במהירות וביעילות עם איש הקשר ו/או מנהל אבטחת המידע מטעם המזמין (ככל והמזמין יבחר למנות מנהל אבטחה), ויפעל בלא דיחוי לפי הוראותיו, ובכלל זה

11.1. הספק ימסור למנהל האבטחה שמטעם המזמין כל מידע ומסמך, מכל מין וסוג, שיידרשו לו כדי להעריך את אמצעי האבטחה שנוקט הספק בקשר עם הסכם זה;

11.2. הספק יאפשר למנהל האבטחה בכל עת גישה לעובדיו המועסקים בביצוע ההסכם, וינחה אותם לשתף עמו פעולה במסגרת תפקידו.

11.3. הספק יפעל בלא דיחוי על פי הנחיות מנהל האבטחה מטעם המזמין, ככל שהוא ימסור הנחיות והוראות כאמור. להסרת ספק – שום דבר בהוראות סעיף זה לא ייחשב כמעביר למזמין את האחריות לאבטחת המידע שעל הספק לקיים על פי ההסכם.

11.4. הספק מתחייב לאפשר לנציגי אבטחת המידע של המזמין ו/או כל גורם הפועל מטעמו, לבצע אצלו (בחצרותיו), מעת לעת ולפי שיקול דעתם, ביקורות (לרבות ביקורות פתע), ביחס לקיום התחייבויותיו על פי ההסכם זה.

11.5. הספק מתחייב להודיע למנהל אבטחת המידע מטעם המזמין על סיום העסקת עובדיו על מנת שהמזמין, יסגור הרשאות גישה לעובדים שסיימו את תפקידם אצל הספק.

12. מבלי לגרוע מהאמור לעיל ולהלן, ידוע לספק שהמידע שהגיע ו/או שיגיע לידיו ו/או לידיעתו בכל צורה שהיא, הוא קניינו ורכושו הבלעדי של המזמין והוא מתחייב בזה להחזיר לידי המזמין, עם סיום ההתקשרות, מכל סיבה שהיא, או מיד עם קבלת דרישה מהמזמין, בכל עת. ידוע לספק כי מסירת המידע ו/או כל חלק ממנו לצד ג' כלשהו עלולה לגרום למזמין נזקים כבדים וחמורים והוא מאשר כי לא יעשה כל פעולה, ובפרט פעולה הכרוכה בהעברה ו/או במסירה של המידע ו/או כל חלק ממנו, אלא על פי היתר מראש ובכתב מהמזמין ועל פי תנאי היתר כאמור.



13. הספק מתחייב כי בסיום ההתקשרות עם המזמין הוא יבער וימחק את כל המידע שקיבל מהמזמין במסגרת מתן השירותים מכל אמצעי בו שמור המידע, ובאופן בו לא יהיה ניתן לשחזר את המידע, ויבער בגריסה כל מסמך הקשור לביצוע השירותים (למעט הסכם זה ומסמכי ההתחשבות הכספית בין הצדדים). בתום 3 ימים ממועד תום ההתקשרות, הספק יעביר תצהיר שיאמת את ביצוע פעולות המחיקה והביעור של כל המידע שהגיע או נצבר במהלך מתן השירותים, בנוסח המאושר על-ידי המזמין.
14. על הספק לאשר, שכל המערכות המוצעות על ידו על כל רכיביהן (תוכנה/חומרה או ציוד אחר) והמתחברים או מופעלים ברשת של המרכז הרפואי, עומדים בתקנים הנדרשים ובין היתר: תקני בטיחות בין לאומיים IEC, תקנים הישראליים, חוק החשמל הישראלי וכדומה. הספק יצהיר כי לכל המאוחר 12 חודשים, מיום חתימה על החוזה, הספק יציג אסמכתא לתהליך הסמכה לתקני אבטחת המידע ISO27799 או ISO27001. כל התקנים יהיו בגרסתם העדכנית ביותר. המרכז הרפואי, שומר לעצמו את הזכות לדרוש מהמציג להציג תעודות עמידה בדרישות כל תקן שהוגדר למערכות, ובכלל זה תעודות הסמכה הניתנות על יד הגוף הרשמי הקובע את התקן הנדרש.
15. חיבור מרחוק יהיה בהתאם לדרישות ולמערכות של מערכות מידע תוך עמידה בתקני ובדרישות אבטחת המידע הנהוגות באתר וללא עלות נוספת.
- כיום תמיכה מרחוק כרוכה ב:

- א. מילוי טפסי פתיחת חשבון, הצהרת סודיות ספק ודרישה לחיבור מרחוק.
- ב. הגעה פיסית של נציג מוסמך של הספק למשרדי מערכות מידע לקבלת הדרכה.
- ג. מדי שנה יבדק עם הספק הצורך שלו בחיבור מרחוק ואם הצורך לא קיים החיבור ייסגר.
- ד. במקרה של נעילת סיסמא, יגיע פיסית של נציג מוסמך של הספק למשרדי מערכות מידע.

על החתום,

רענן עייש  
מנהל סייבר והגנת הפרטיות  
מרכז רפואי ברזילי.