



## **אגף מערכות מידע ומחשוב**

### הנחיות אבטחת מידע מרכז רפואי ברזילי

- 1.1. כללי
- 1.2. בקרת גישה על המערכות
- 1.3. בקרת הרשאות
- 1.4. אבטחת תקשורת
- 1.5. הגנת תחנות קצה
- 1.6. ניהול משתמשים
- 1.7. אבטחה פיזית
- 1.8. הגנה על פריט מידע
- 1.9. גיבוי מידע
- 1.10. המשכיות עסקית

### תנאי סף מקצועיים למציע:

- על המציע להחזיק בהסמכה ISO/IEC27001 בתוקף למשך כל תקופת ההתקשרות עם המזמין.
- על המציע להחזיק בהסמכת כשירות הסייבר בשרשרת האספקה רמה A מטעם מערך הגנת הסייבר לפי תהליך ותנאים בנתיב הבא :  
<https://www.gov.il/he/departments/news/queriesupply>
- הספק ערוך ומתחייב להעמיד שירות לפי דרישות מסמך זה גם בתנאים ובעת שעת חירום או אירוע סייבר בהתאם ליעדי השירות המוגדרים בהסכם שירות (SLA), ובכלל זה יוגדר כמפעל חיוני לצורך הפעלת ריתוק משקי על עובדיו המעורבים במתן שירות.
- לספק קיים אתר החלופי (אתר DR) אחד לפחות, באופן שתוקטן ההסתברות לכך שהאתר החלופי והאתר הראשי יושפעו באופן דומה מתרחיש מסוים בשעת חירום, בכלל זה, השפעה על מרכיבי התשתית הפיזית (חשמל, תקשורת וכד') המשמשים את האתרים.
- על הספק לעמוד בהוראות חוק הגנת הפרטיות.
- הספק מתחייב שלא להקים מאגר נתונים ולא לשמור נתונים הודות מטופלים ובדיקות ולמחוק את המידע כולל ברשימות הלוגים ומכל מקום אחסון אחר, לאחר חודש ממסירת תוצאות הבדיקה לארגון המבקש את הבדיקה, ארגון המבקש את הבדיקה יוכל להאריך את משך שמירת המידע.
- הספק מתחייב לאפשר למנהל אבטחת מידע או כל גורם אחר מטעמם לבצע בדיקה אבטחת מידע בתיאום מראש בחצרותיו.
- הספק מתחייב לעדכן את המרכז הרפואי בכל שינוי משמעותי בתהליך המחשוב, רשת ותקשורת הבדיקות.
- הספק מתחייב שלא להעביר מידע מחוץ לגבולות המדינה או למסור אותו לגורם אחר ללא רשות המרכז הרפואי .
- הספק יפרט את תכנית ודרישות התשתיות המלאה הנדרשת להתקנת הציוד המוצע על ידו. התוכנית תציין את מהלך צנרת ותעלות החשמל והתקשורת הנדרשים, ההזנות הנדרשות לציוד, עומסי החשמל, צריכת התשתיות [הספק, ספיקה, מתח, זרם, טמפ', לחץ וכד'].
- הספק יאשר שכל המערכות המוצעות על ידו על כל רכיביהן, עומדות בהנחיות משרד הבריאות ובתקני האיכות והבטיחות הנדרשים ובין היתר: תקני אבטחת מידע בין לאומיים (גם בענף) HIPAA , GDPR , ISO/ IEC27018 תקנים ישראלים כגון אמ"ר , הגנת הפרטיות ו- ISO 27799 .

- כל התקנים יהיו בגרסתם העדכנית ביותר, ביה"ח שומר לעצמו את הזכות לדרוש מהמציג להציג תעודות עמידה בדרישות כל תקן ועמידה בהנחיות הרגולטור שהוגדר למערכות ובכלל זה תעודות הסמכה הניתנות על יד הגוף הרשמי הקובע את התקן הנדרש.
- יפורטו דרישות תשתית תקשורת מחשבים למערכת ולכל אחד ממרכיביה.
- יפורטו דרישות נפחי האחסון, גודל הקבצים והפורמט שלהם ופרק הזמן שהם ישמרו בשרתי מרכז רפואי ברזילי.
- שמירת מידע בענן – המציע יפרט בהצעתו ויספק את כל המסמכים הדרושים שתומכים באופן שמירת המידע בענן, נפחי האחסון, שיטות ההצפנה על מידע בתנועה ומנוחה וכן הבקורות שבהם מגן ספק הענן מפני זליגת מידע בהתאמה לחוזר משרד הבריאות "שימוש במחשוב ענן במערכת הבריאות 2/2021".
- יפורטו דרישות שרתים שיכללו כמות ה-cores (מעבדים), (memory) זיכרון ונפחי האחסון וכן עלויות ותשתית הוספת עמדות מחשוב וציוד מחשוב נלווה.
- התחייבות שמתן שירות באתר המרכז הרפואי ברזילי, לא יותנה בחיבור מרחוק.
- באם נדרש להפעיל ציוד קצה לצורך הפעלת המערכת או חיבור למערכות בית החולים:
  - כל הציוד יסופק ע"י הספק וללא עלות נוספת.
  - הספק לא יתקין רכיבי חומרה שלא הוצגו באיפיון או יחבר מערכות בקרה לאינטרנט, גם לא למתן תמיכה, ללא אישור של אגף מערכות מידע ובהנחייתו.
  - על מחשבי הניהול של מערכות הבקרה, יהיה ניתן להתקין ANTIVIRUS שיעודכן באופן שוטף ובגירסתו המעודכנת ביותר ועל בסיס אישור מייצרן.
  - המערכת תותאם באופן מלא לעבודה על מערכת הפעלה חלונות 10 ותשודרג במסגרת תקופת ההתקשרות לעבודה בפלטפורמות חדשות של מערכות הפעלה העתידיות.
  - הספק יספק ספרות טכנית ותפעולית מלאה של כל הציוד לפחות 5 העתקים ו-3 מדיות דיגיטליות.
  - הספק יספק מפרט מלא של הממשקים ואופן פעולתם ב-3 מדיות דיגיטליות.

## 1. דרישות הסייבר

### 1.1. כללי

- 1.1.1. כל ספק הנותן שירותים בנושא המחשוב חייב לעמוד בדרישות המוגדרות בפרק זה.
- 1.1.2. מטרת הפרק להגדיר ולקבוע את ההוראות וההנחיות שיחייבו את הספק ואת כל מי מטעמו שיועסק במתן השירותים, כחלק מכלל הפעולות, הנקטות בכדי להגן על מידע של המרכז הרפואי ומערכות בקרת המבנה של המרכז הרפואי.
- 1.1.3. האמור בפרק זה הינו תנאי מחייב לביצוע השירותים.
- 1.1.4. מוסכם ומוצהר כי ההתחייבויות שבסעיף זה, יעמדו בתוקפן גם במקרה של סיום או ביטול ההתקשרות לתקופה של 7 שנים מתום תקופת ההתקשרות בהסכם ההתקשרות.
- 1.1.5. תיושם אבטחת מידע כמוגדרת בתקן ISO-27001 : שמירה על סודיות, שלמות ואמינות, זמינות ושרידות המידע במערכות המידע של הספק ומי מטעמו. כל זאת בכפוף לתקנות הגנת הפרטיות ולחוקי אבטחת מידע.
- 1.1.6. עמידה בחוקים, תקנות והנחיות המתפרסמות מעת לעת על ידי מנכ"ל המשרד, רמ"ט ומחלקת אבטחת מידע במשרד הבריאות.
- 1.1.7. הספק יציית לחוק הגנת הפרטיות התשמ"א – 1981 ולתקנות הגנת הפרטיות 2017.
- 1.1.8. ייעשה שימוש במגוון שיטות וכלים טכנולוגיים להבטחת שלמות ואמינות הנתונים המועברים בין רכיבים שונים של מערכת, בין מערכות בתוך הארגון (ממשק פנימי) ומהארגון החוצה (ממשק חיצוני).
- 1.1.9. הספק יהיה אחראי כלפי המרכז הרפואי על כל המידע המועבר אליו או דרכו, לרבות דוחות, טפסים, קבצים מגנטיים, מידע לגבי נתונים אישיים ומערכות מידע של המזמינה.
- 1.1.10. הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי מכרז זה, ויציג למזמין, על פי דרישתה, את אמצעי אבטחת החומר.
- 1.1.11. הספק יתחייב לשמור בסודיות מלאה כל נתון ו/או מידע שהגיעו אליו במסגרת ביצועו של חוזה ההתקשרות לביצוע פרויקט זה, בין במישרין ובין בעקיפין ולא יגלה כל נתון ו/או מידע כאמור לכל צד שלישי שהוא.
- 1.1.12. כמו כן מתחייב הספק לגרום לכך שכל המועסקים על ידו בביצוע הסכם ההתקשרות למתן שירות עבור המזמין יחתמו על התחייבות לשמירת סודיות. הספק יצהיר שידוע לו שאי מילוי התחייבויותיו לפי סעיף זה מהווה עבירה על פי חוק העונשין, התשל"ז - 1977 ועבירה על חוק הגנת הפרטיות, התשמ"א - 1981.
- 1.1.13. הספק אינו רשאי לעשות שימוש שלא לעניין מילוי מחויבויותיו בגין מכרז זה במידע מכל סוג שיגיע אליו במסגרת עבודתו, לרבות מידע אודות הציווד לסוגיו, מידע סטטיסטי אודות השירות וכל מידע אחר.

- 1.1.14 עם סיום ההתקשרות יחזיר הספק למזמין את כל החומר האמור, או ישמידו לפי הוראת המזמין.
- 1.1.15 הספק מתחייב לבצע פיתוח ככל שנדרש על פי נוהל הפיתוח המאובטח הארגוני ועל פי מתודולוגיית תכנון ופיתוח (כולל עמידה של אנשי צוות הפיתוח בתקנים ובדיקות) בצורה מאובטחת.
- 1.1.16 הספק מתחייב לעמוד בדרישות אבטחת המידע של המרכז הרפואי .
- 1.1.17 הספק ידאג לאבטחת כל המידע אשר יגיע אליו במסגרת מכרז זה. הספק אף יגן על המידע מפני כל נזק, לרבות גניבה, שריפה וכד'.
- 1.1.18 הספק ימנע גישה למערכות המחשב שברשותו, או למערכות המחשב המשרתות אותו, ממי שאינו מוסמך לעיין בחומר או במידע המאוחסן במחשב, או ממי שלא חתם על התחייבות לשמירת סודיות.
- 1.1.19 הכניסה למערכות המחשוב של המרכז הרפואי ברזילי, תתבצע באמצעות גישת MFA מאובטחת, באמצעות כרטיס חכם ו/או רכיב ביומטרי ו/או OTP ו/או PNA עפ"י החלטת המרכז הרפואי.

## 1.2 בקרת גישה על המערכות

### 1.2.1 גישה למערכות המזמין

1.2.1.1 אימות המשתמש בהתחברותו למערכות המרכז הרפואי, תעשה באמצעות חשבון משתמש יעודי, סיסמה שתוחלף בהתאם למדיניות המרכז הרפואי ואימות כפול.

1.2.1.2 הזדהות המשתמש מול משאבי המזמין תהיה באמצעות MFA – סיסמה + כרטיס חכם ו/או רכיב ביומטרי ו/או OTP בתצורת Secured Desktop.

1.2.1.3 גישה אל משאבים הרלוונטיים של המזמין תינתן לעובדי ספק המורשים בלבד.

### 1.2.2 גישה למערכות הספק

1.2.2.1 לא תהיה אפשרות לגישה אונימיית למשאבי מיגע של הספק.

1.2.2.2 בקרת גישה למערכות מידע תיושם עפ"י מהות התפקידים.

1.2.2.3 גישת המשתמש אל המערכות המידע לא תהיה ישירה אלא רכיבי הגנה, כדוגמת באמצעות-Terminal Server, WAF, PROXY וכו' לפי העניין.

## 1.3 בקרת הרשאות

1.3.1 הרשאות למשתמשי המערכות תינתנה עפ"י עקרונות "המינימום הנדרש" (Least Privilege) בהתאם לאפיון התפקיד ובאישור בעל המידע בכל מערכת.

1.3.2 עם שינוי ו/או הסבת תפקידו של בעל החשבון כלל ההרשאות הקודמות יבוטלו וינתנו עפ"י הפרופיל החדש.

1.3.3 במקרה של סיום/הפסקת העסקה של עובד ו/או אצל הספק גישה למערכות תחסם באופן מיידי

1.3.4 מתן כל הרשאות גישה מותנית תהיה בתנאי בחתימת העובד על הצהרת שמירת הסודיות.

## 1.4 אבטחת תקשורת

### 1.4.1 תשתיות תקשורת LAN

1.4.1.1 כלל תשתיות תקשורת יופרדו ככל הניתן ברמה פיזית ל-2 דומיינים IT – Information Technology ו-Operational Technology.

1.4.1.2 חיבור ו/או התממשקות בין ה-IT ל-OT, ככל שנדרש, יהיה באמצעות רכיב אבטחה ייעודי בשכבות גבוהות ודרך FW ייעודי.

1.4.1.3 הספק נדרש להפעיל מערכת הגנת בקרת גישה למשאבי רשת NAC לכלל מרכיבי הרשת, בתצורה של אכיפת "תביעת אצבע" לכל סוג רכיב.

1.4.1.4 תשתית אקטיבית תמוקם בארונות תקשורת ייעודיים נעולים פיזית ובאופן שמונע

אפשרות גישה לא מורשית לציוד.

1.4.2. כלל רשתות ה-LAN יופרדו זו מזו ככל הניתן באמצעות FW .

### 1.5 הגנת תחנות קצה

1.5.1. מערכות הפעלה תהינה מתוחזקות, מעודכנות ומסונכרנות, בהתאם לפרסומים רשמיים של יצרניהן.

1.5.2. תחנות קצה יהיו מוגנות באמצעות מערכות EPS או אנטי וירוס. עדכוני גרסאות ומקורות מידע יהיו מתוזמנות עם יצרניהן.

1.5.3. תחנות קצה ינוהלו ע"י הספק באופן מרכזי כולל ניהול סיסמאות, יהיו בדומיין בעל מדיניות הקשחה שבא למזער את חשיפת המשתמש לחולשות אבטחה ידועות ולא ידועות.

1.5.4. יישומים מובנים בתוך מערכת ההפעלה שלא נחוצים יחסמו.

1.5.5. דפדפני האינטרנט יוקשחו לפי המדיניות הארגונית.

1.5.6. אחר 15 דקות של חוסר שימוש, התחנה תיכנס למצב שומר מסך.

### 1.6 ניהול משתמשים

1.6.1. הקמת חשבון המשתמש עבור השרות, עדכונו וביטולו יבוצע ב-AD של בדומיין המקומי של הספק בקבוצה ייעודית עפ"י מדיניות ניהול המשתמשים של הספק.

1.6.2. במקביל, על הספק יגיש בקשה למזמין לצורך להקמת/גרירת חשבון המשתמשים במערכות הרלוונטיות של המזמין, ככל שנדרש, לצורך מתן שרות. הנ"ל עפ"י נוהל ניהול משתמש של המזמין.

1.6.3. ניהול חשבונות משתמשים מסוג Local Admin יהיה מרכזי באמצעות Microsoft LAPS או דומה.

1.6.4. במקרה של סיום/הפסקת העסקה של עובד ו/או אודבן ו/או חשד לגניבה של סיסמאות של העובד המורשה, מנהל האתר או בר כוחו יהי אחראי לביצוע ותיעוד, בין היתר, פעולות הבאות:

1.6.4.1. דיווח מידי למזמין ולמנהל המערכת על המקרה, לצורך ביטול חשבון המשתמש במערכות המזמין.

## 1.7. אבטחה פיזית

### 1.7.1. אחריות

1.7.1.1. עובדי הספק יהיו אחראים על ליווי אורחיהם ותשומת לב לאורחים לא קרואים.

1.7.1.2. באזורים רגישים, על מנהל האתר לוודא קיומן של הבקורות הבאות:

1.7.1.2.1. קירות חיצוניים מוצקים וכל הדלתות החיצוניות מוגנות היטב בפני גישה בלתי מורשית, באמצעים כגון: מנגנוני בקרה, מנעולים ומערכות אזעקה.

1.7.1.2.2. דלתות בקרת אש על פי דרישות תקן הבטיחות.

1.7.1.2.3. מחסומים פיזיים באזורים המכילים ציוד מחשוב רגיש, כדי למנוע כניסה בלתי מורשית וסכנות סביבתיות העלולות להיגרם כתוצאה משריפה או הצפה.

1.7.1.2.4. חלונות חדר המחשב ו/או תקשורת יהיו מסורגים וסגורים באופן שתהייה הגנה על זוגיות החלון מפני ניפוץ, ובנוסף תותקן מערכת אזעקה.

1.7.1.2.5. חלונות חדר המחשב ו/או תקשורת יהיו מסורגים וסגורים באופן שתהייה הגנה על זוגיות החלון מפני ניפוץ, ובנוסף תותקן מערכת אזעקה.

1.7.1.2.6. חלונות חדר המחשב ו/או תקשורת יהיו מסורגים וסגורים באופן שתהייה הגנה על זוגיות החלון מפני ניפוץ, ובנוסף תותקן מערכת אזעקה.

1.7.1.2.7. באזורים רגישים יהיו אמצעי כיבוי אש כגון: מטפים, מערכות התזת מים ומערכות גילוי עשן.

1.7.1.3. שרתי המערכת ויתר ציוד הליבה יוגנו מפני הפסקות חשמל באמצעות מערכות אל פסק.

1.7.1.4. תותקן תאורת חירום במקומות מרכזיים אשר תפעל בעת הפסקת חשמל.

### 1.7.2. אבטחת משרדים, חדרים ומתקנים



- 1.7.2.1 חדרים המכילים מידע ינעלו בעת היעדרות העובד מחדרו ובעזבו את החדר בסיום יום העבודה.
- 1.7.2.2 כל מידע רגיש בהיבט עסקי או של צנעת הפרט ישמר בארון נעול או בכספת כל עוד לא נעשה בו שימוש או כאשר העוסק בו אינו בקרבתו.
- 1.7.2.3 חדרים המכילים חיווט או ציוד תקשורת כגון ארונות חיווט ומערכות טלפוניה יהיו נעולים תמיד והגישה אליהם תוגבל לעובדים מורשים בלבד.
- 1.7.2.4 דלתות האזורים הרגישים יהיו נעולות תמיד. כניסה לגורם מאושר תתאפשר על ידי תג כניסה או מפתח.
- 1.7.2.5 לא יהיה סימון המשמש אינדיקציה למיקום מחשבים או מרכזי תקשורת על מנת לא למשוך את תשומת ליבם של בלתי מורשים.

#### 1.8 שמירת מידע רגיש

- 1.8.1.1 יש איסור מוחלט לשמור מידע של המזמין בתחנות עבודה או במערכות ללא אישור אבטחת מידע של המזמין.
- 1.8.1.2 גישה למידע של המזמין במערכות המזמין תהיה אך ורק לנותני שירותים שאושרו על ידי מחלקת אבטחת מידע וסייבר של המזמין.
- 1.8.1.3 השירות יסופק מאתר הממוקם בתחומי מדינת ישראל.
- 1.8.1.4 הספק מאשר ללא תנאי מקדים לבצע מבדק ו/או בקרה ע"י המזמין ו/או מי מטעמו בנושאים כדלהלן:
- 1.8.1.4.1 תשתיות וארכיטקטורה
- 1.8.1.4.2 תהליכי העברת מידע
- 1.8.1.4.3 נוהלי אבטחת מידע
- 1.8.1.5 הספק מתחייב ליישם את המלצות ע"פ הדו"ח שיופק מהמבדק.
- 1.8.1.6 כול חריגה מיישום ההמלצות מחייב אישור אבטחת מידע של המזמין.
- 1.8.2 **התחייבות לשמירה על סודיות** – באחריות הספק להחתים את העובדים מטעמו על טופס שמירה על סודיות.
- 1.8.3 **ניהול מדיה דיגיטלית** - מדיה הכוללת מידע של המזמין צריכה להיות מוגנת פיזית או שהמידע שבה יוצפן, נדרש לנטר מצבה ומיקומה של מדיה הכוללת מידע של המזמין לא מוצפן.

1.8.3.1. מדיה מנוידת הכוללת מידע פרטני תוגן מפני גישה בלתי מורשית, באמצעות הצפנת המידע.

1.8.3.2. ככל שהדבר רלוונטי, מעגל הגנה ראשון לרכיבי טכנולוגיית המידע יהיה מעגל אבטחה פיזי.

#### 1.9. גיבוי מידע

1.9.1. הספק נדרש לגבות את כל המערכות המעורבות במתן שירות למזמין בתוך גבולות של מדינת ישראל.

1.9.2. אופן הגיבוי למערכות מידע ייקבע ע"י מדיניות גיבויים של הספק ומבלי לפגוע מדרישות מסמך זה.

1.9.3. כל יום יבוצע גיבוי למידע.

1.9.4. באתרים בהם מבוצעים גיבויים דיפרנציאליים או אינקרמנטליים, יבוצע בכל מקרה גיבוי מלא לפחות אחת לשבוע.

1.9.5. גיבוי למערכות קריטיות בין היתר יהיה גיבוי חם, קרי זמינות מידית.

1.9.6. מספר מחזורי גיבוי בכל אתר ייקבע ע"י ועדת ההיגוי לאבטחת מידע, ובכל מקרה מספר מחזורי הגיבויים לא יפחת מ- 18 כדלהלן:

1.9.6.1. 7 מחזורים יומיים.

1.9.6.2. 4 מחזורים שבועיים.

1.9.6.3. 6 מחזורים חודשיים.

1.9.6.4. 1 מחזור שנתי.

1.9.7. עותק של הגיבוי הרבעוני יוחזק באופן מאובטח באתר מרוחק (אתר DR) מהאתר בו ממוקמות מערכות.

1.9.8. עותק של גיבוי חודשי יועבר באופן מאובטח לרשות המזמין ויוחזק באתר שלו.

#### 1.10. המשכיות עסקית

1.10.1. כתנאי מקדים להפעלת פעילות הספק יגיש לאישור המזמן את תכנית המשכיות עסקית שכוללת לפחות נושאים הבאים:

1.10.1.1. **משאבי אנוש** - בהתבסס על ניתוח ההשלכות העסקיות, יוגדרו תחומי האחריות והסמכות, לחברי ההנהלה, צוותי עבודה, נותני שירותים פנימיים וחיצוניים,

וגורמים אחרים. כמו כן, תיבנה תכנית גיבוי לכ"א חיוני ויוגדר צוות מקצועי לניהול והפעלת התהליכים והשירותים החיוניים בעת חירום, לרבות במקרה של שביתה, אסון טבע, אירוע בטחוני, מגפה ו/או פנדמיה וכיו"ב.

1.10.1.2 **נושאים טכנולוגיים** - תכנית ההמשכיות העסקית תתייחס לכל מרכיבי הטכנולוגיה הנדרשים לשמירת הרציפות העסקית ו/או לאישוש הפעילות.

1.10.1.3 **העתקת תהליך או שירות חיוני** - תכנית המשכיות העסקית תיתן ביטוי להעתקת תהליך או שירות חיוני למיקום חדש.

1.10.1.4 **חלופות עבודה ידנית** - תכנית ההמשכיות העסקית תכלול, בהתאם לעניין, נהלים לביצוע תהליכי עבודה ידניים, אשר אושרו מראש על ידי הנהלת הספק, כחלופה לתהליכים ושירותים חיוניים. בהקשר זה, הספק ידאג לגיבוי רשומות מידע של המזמין.

1.10.1.5 **גיבוי נתונים** – כמפורט בסעיף 1.9 לעיל.

1.10.1.6 **תקריות אבטחת מידע** - תפותח מדיניות תגובה לאירועי אבטחת מידע אשר תשולב בצורה נאותה בתכנית ההמשכיות העסקית. במקרה של פריצת מעגלי ההגנה, אלמנט מרכזי בתגובה לאירוע אבטחת מידע הוא חלוקת האחריות להערכה, לתגובה ולניהול אירועי האבטחה ופיתוח קווים מנחים לעובדים בנוגע לנוהלי הסלמה ודיווח. הספק נדרשת לקבוע מי יהיה אחראי להכריז על תקרית, ומי אחראי לשחזר את מערכות המחשב שנפגעו מרגע שהתקרת הסתיימה. מי שמוטלת עליו אחריות זו צריך להיות בעל המומחיות הנדרשת כדי להגיב בדרך מהירה ונאותה

1.10.1.7 **מדיניות "גישה מרחוק"** - נהלי עבודה לגישה מרחוק יהיו חלק מתכנית ההמשכיות העסקית, שכן באירועי חירום מסוימים לא תתאפשר גישה לחלק ממתקני הספק, ולכן עלול לעלות צורך במתן גישה מרחוק לעובדים או נותני שירותים חיצוניים. מדיניות הגישה מרחוק תאושר ע"י ההנהלה הבכירה ותתייחס לסיכונים הכרוכים במדיניות ולקיום מנגנוני בקרה ואבטחת מידע הולמים.