



גישה של נותן שירות חיצוני לרשת הטכניון

1. רקע

כל חיבור מרחוק אל רשת הטכניון והשתלטות על מערכת מידע כלשהי מהווה סיכון פוטנציאלי לרשת הטכניון כולה ולמשתמשים המחוברים אליה. על מנת לצמצם את רמות הסיכון למינימום האפשרי, אגף מחשוב ומערכות מידע בוחן ומטמיע פתרונות טכנולוגיים שונים על בסיס קבוע.

2. מטרת הנוהל

להסדיר את הנושא של מתן גישה של נותן שירות חיצוני למערכות מידע הממוקמות ברשת הטכניון.

3. הגדרות

RDP – אמצעי להתחברות ועבודה מרחוק במערכות Microsoft.
SSH – אמצעי להתחברות ועבודה מרחוק במערכות Linux.
TeamViewer – אפליקציה להתחברות מרחוק.

4. סמכות ואחריות

- 4.1 באחריותם של מנהלי המחלקות/מדורים באגף מחשוב ומערכות מידע לפעול בהתאם לאמור בנוהל זה.
- 4.2 בסמכות הממונה על אבטחת מידע של הטכניון לבחון דרכים אחרות של מתן השירות ע"י נותן השירות. במידה ותהיה דרך אחרת לספק את השירות הנדרש ללא חיבור מרחוק אל רשת הטכניון, החיבור של נותן השירות לא יאושר.

5. שיטה

5.1 אישור גישה מרחוק

- 5.1.1 על מנהל מחלקה/מדור באגף מחשוב ומערכות מידע לקבוע האם הכרחית התחברות מרחוק ומתן שירות למערכת מידע כלשהי במחלקה/מדור שהוא ממונה עליו.
- 5.1.2 במידה ויש צורך אמיתי שנותן שירות חיצוני יתחבר מרחוק וייתן שירות למערכת מידע באגף מחשוב ומערכות מידע, על מנהל המחלקה/מדור להודיע על כך לממונה אבטחת מידע של הטכניון על מנת לבחון את אופי ההתחברות והערכת סיכונים בחשיפת המידע.
- 5.1.3 על מנהל המחלקה/מדור באגף מחשוב ומערכות מידע לקבוע תאריך תוקף לבקשה. תאריך התוקף יוגבל למקסימום של שנה מיום מתן האישור. במידה ונותן השירות לא סיים את עבודתו בפרק הזמן שהוקצב לו, על מנהל מחלקה/מדור להודיע על כך לממונה על אבטחת המידע במטרה להאריך את תקופת ההתחברות.

5.2 מתן גישה מרחוק

- 5.2.1 התחברות של ספק חיצוני למערכת מידע ברשת הטכניון תתבצע באחת משתי הדרכים הבאות:
- א. במידה ולנותן השירות יש כתובת IP קבועה, הגישה למערכת תתבצע ישירות מכתובת ה-IP של נותן השירות אל המערכת באמצעות שירותי RDP, SSH למערכות Windows, Linux בהתאם.



- ב. במידה ואין ברשות נותן השירות כתובת IP קבועה, החיבור לרשת הטכניון יתבצע באמצעות VPN ולאחר מכן תתבצע ההתחברות למערכת.
- ג. במקרה של צורך לקבל שירות מיידי מנותן השירות, ניתן להשתמש באפליקציה TeamViewer אשר נרכשה לצרכי השתלטות על מערכות. תנאי הכרחי לשימוש בפתרון זה: על מקבל השירות להיות מול המחשב/שרת בזמן ההתחברות של ספק השירות ולוודא שנותן השירות התנתק בסיום העבודה.
- 5.2.2 כל גישה של נותן השירות לרשת הטכניון מרחוק המתוארת בסעיף 5.2.1 א ו-5.2.1 ב, תחויב בחתימתו על הצהרת שמירה על סודיות אשר תגובש ע"י הלשכה המשפטית של הטכניון בהתאם לאופי השירות ורמת החשיפה למידע רגיש.
- 5.3 סיום ההתקשרות עם נותן השירות
- 5.3.1 בעת סיום ההתקשרות עם נותן השירות, על מנהל מחלקה/ראש מדור להודיע על כך לממונה על אבטחת המידע.
- 5.3.2 במידה וסופק לנותן השירות ציוד נלווה כדי להתחבר מרחוק, על מנהל מחלקה/ראש מדור לדאוג להחזרתו.
- 5.3.3 באחריות מנהל המחלקה/ראש מדור להעביר את הציוד המוחזר לממונה אבטחת המידע.
- 5.4 תיעוד ובקרה
- 5.4.1 ממונה על אבטחת המידע ינהל רשימה של נותני השירות המורשים לגשת מרחוק אל רשת הטכניון, כולל תאריך תחילה וסיום.
- 5.4.2 בסיומה של תקופת השירות אשר הוגדרה ע"י מנהל מחלקה/מדור באגף מחשוב ומערכות מידע, **אפשרות** החיבור לרשת הטכניון עבור נותן השירות תבוטל.

6. תכולה ותוקף

- 6.1 נוהל זה חל על כל מחלקות אגף מחשוב ומערכות מידע.
- 6.2 תוקף נוהל זה חל מיום פרסומו.

7. שינויים בנוהל

מהדורה	תאריך תוקף	נכתב ע"י	מהות השינוי	אושר ע"י
1.0	24.12.2013	קאופמן אלכסנדר	גרסת בסיס	אהרוני אשר

אשר אהרוני
ראש אגף מחשוב ומערכות מידע