



## עדכון חשוב – אבטחת שירותי ArcGIS Online

### לכל לקוחותינו:

חברת Esri מחוייבת לתקני אבטחת המידע המחמירים הנהוגים כסטנדרט בשוק, וזאת על מנת לספק לכם שירות טוב יותר וסביבת יישומים בטוחה יותר. סטנדרטים כאלו מחייבים מפעם לפעם עדכונים שוטפים. בתחילת חודש פברואר 2019 צפוי עדכון משמעותי לתקני האבטחה של שירות המיפוי הענני ArcGIS Online, שעשוי להיות בעל משמעות עבור רובכם, ולכן מצאנו לנכון לפנות אליכם בהודעה זו ולוודא כי אתם מבצעים את הפעולות הנדרשות על מנת שתהליכי העבודה שלכם לא יופרעו מהשינוי.

- **המהות:** בתחילת פברואר 2019 תוסר התמיכה מפרוטוקול האבטחה TLS 1.0,1.1 מפורטל ArcGIS Online, ותשאר התמיכה רק בפרוטוקול TLS 1.2.
- **הסיבה לשינוי:** גרסאות ישנות של הפרוטוקול הן בנות למעלה מעשור, וגופי תקינה בינ"ל לאבטחת מידע דורשים שהתמיכה בהן תפסק על מנת ששירותי ענן (כגון AGOL) ימשיכו להנות מתקינה (ומאליו גם מאבטחה משופרת).
- **המשמעות למערכות GIS קיימות:** כל מוצר שמתקשר עם ArcGIS Online, בין אם למטרות פרסום שירותים, טעינת Basemaps, גישה לשכבות מתוך AGOL / Living atlas, או שימוש בשירותי AGOL מקוונים (כגון routing, geocode), עובר דרך הפרוטוקול הזה, וצריך להיות מותאם לשימוש בגרסה 1.2. אם לא יהיה מותאם - לא יוכל לתקשר לשירותים הנ"ל החל מפברואר 2019.
- **אילו מוצרים מושפעים:** כל מוצרי ArcGIS, כולל תוכנות Desktop, Enterprise וסביבות פיתוח, יתאמו החל מגרסה מסויימת לפרוטוקול המעודכן. לקוחות יוכלו לשדרג את מערכתיהם לגרסה תואמת או – אם אין ביכולתם לשדרג את הגרסה – להתקין טלאי תוכנה יעודי) או להפעיל capability שאינו דולק כברירת מחדל במקרים מסויימים (שיאפשר את ההתקשרות עבור הגרסאות הקיימות).
- **מה עליכם לעשות כדי להתכונן לעדכון המדובר:** על מנת שעבודת המוצרים השונים לא תופרע, יש להשלים לפני פברואר 2019 את הצעדים המפורטים בתחתית הקישור הבא: <https://support.esri.com/en/tls>, לפי גרסת מוצרי ArcGIS שברשותכם ו/או גרסת מערכת ההפעלה על גביה הם מותקנים.

מידע נוסף תוכלו למצוא בקישור הבא: <https://www.esri.com/arcgis->

[blog/products/product/administration/2019-arcgis-transport-security-improvements/](https://www.esri.com/arcgis-blog/products/product/administration/2019-arcgis-transport-security-improvements/)

