Memorandum

MEL Cyber Task Force

The MEL Cyber Task Force is proud to present Version 2 of its Cyber Risk Management Program.

Version 2 does not change many previously present items in Tiers 1 or 2, but offers more clarity and adds a Tier 3 for full deductible reimbursement. PLEASE NOTE, any members already in compliance with either Tier 1 or Tier 2 prior to March 8, 2021 will have their compliance grandfathered until January 1, 2022. As always, you must be in compliance with the tiers at the time of the claim in order to be eligible for reimbursement; review the Deductible Reimbursement Application for details.

Following are the most notable changes in Version 2 of the Cyber RMP you should be aware of. Please review all details of the Cyber RMP to ensure you meet compliance.

Cyber Awareness Training (Tier 1)

✓ Training of one (1) hour must occur on an annual basis, versus the bi-annual basis required in the old RMP.

Password Strength (Tier 1)

✓ This requirement has been moved from Tier 2 to Tier 1, and a Password Policy is required to be adopted.

Email Warning Label (Tier 1)

✓ An automatic email warning label must be added to all emails coming from outside your organization.

Government Cyber Memberships (Tier 1)

✓ This is a new requirement whereby the member will have to register with NJCCIC and MS-ISAC.

System & Event Logging (Tiers 2 & 3)

✓ This is a new requirement whereby logs should be applied throughout your network (Tier 2) and reviewed regularly (Tier 3).

Remote Access (Tiers 2 & 3)

✓ This is a new requirement where Virtual Private Network (VPN) will be required for all remote access (Tier 2) and Multi-Factor Authentication is deployed (Tier 3).

Banking Controls (Tier 2)

✓ This is a new requirement whereby the member will deploy certain controls to ensure safe banking.

IT Business Continuity Plan (Tier 2)

✓ This is a new requirement whereby the member will have to create a continuity plan for Information Technology. This should be a part of the Continuity of Government plan.

Tier 3

✓ Tier 3 is our enhanced security tier, requiring practices like network segmentation, Multi-Factor Authentication (MFA), vendor security audit and password integrity checks.