Table of Contents

1.0 INTRODUCTION

Under the NERC functional model, ATURA POWER's Generating Stations are registered as a Generator Owner (GO) and Generator Operator (GOP) in the NPCC region within the IESO control area. As such, ATURA POWER is accountable to protect the Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability on the BES.
The purpose of this policy is to describe what action shall be taken by Suppliers in order to meet the requirements of 'NERC CIP-003: Cyber Security – Security management Controls', pertaining to 'Transient Cyber Assets and Removable Media malicious code risk mitigation'.

2.0 DEFINITIONS

Bulk Electricity System (BES): The electrical generation resources, transmission lines, interconnections with the neighboring systems and associated equipment, generally operated at voltages of 100 kV or higher.

CIP: Critical Infrastructure Protection

Supplier: An outside source hired by the Company to complete the work

Transient Cyber Asset (TCA): A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

3.0 REFERENCES

3.1 NERC CIP-003: Cyber Security – Security management Controls
3.2 NERC Glossary of Terms

4.0 SECURITY PATCHES

The Supplier **Shall** have their Transient Cyber Assets updated with all security patches that were released at least up to six (6) months prior to connecting to ATURA POWER Cyber Systems. ATURA POWER understands that patches require testing and is of the view that any patches released six (6) months prior would provide sufficient time to review and install.

5.0 ANTIVIRUS SOFTWARE

The Supplier **shall** have their Transient Cyber Assets antivirus software updated with virus definition that were released at least up to two (2) weeks prior to connecting to ATURA POWER Cyber Systems.

6.0 SCAN RESULTS

The Supplier **shall** provide the scan results of the Transient Cyber Asset or removable media to be connected to ATURA POWER Cyber Systems showing the virus definition date and a virus and malware free system, where the scan was run at most two (2) weeks prior to connecting to ATURA POWER Cyber Systems.