Seneca Falls Central School District

Communicating Internal Control Related Matters Identified in an Audit

Management Letter (For Year Ended June 30, 2018)

Current Year Deficiencies in Internal Control and Corrective Action Plan

I. **Employee Reimbursements**

The district was found to have provided a cell phone stipend that is not approved through the board of education minutes or an employee's contract. The District will begin to ensure that all contracts as well as Memorandum of Agreements are shared with the Central Business Office. Contracts and Memorandum of Agreements will be checked to ensure any stipends to the specific employee are included in the language.

II. **Disbursements**

The District was found to have five instances in which the purchasing agent did not approve the voucher for payment to a referee. All athletic official vouchers are now being re-routed to the Business Office for approval before payment.

III. **Receipts**

The District was discovered to have had three instances in which deposits were not made to the bank in a timely manner. Details were not available on which receipts were in question. We currently have two instances in which students pay for programming prior to the program starting (i.e. Advanced Placements Assessments and Drivers Education costs). The District will review the collection process with all stakeholders (Central Business Office, District Business Office, building administrators and building office staff) to ensure a timely collection and deposit of the funds within the 3-5 business day deadline.

IV. **Cyber Risk Management**

The District currently has an Information Security Breach and Notification Policy #5686. This policy, as well as all District policies, are currently being re-written. This information breach policy language will include cyber risk management language once updated. Currently the District has completed the following assessments and enhancements to protect against said threats:

a. July 2018: Upgrade to iBoss internet filter which removed several outgoing open ports
b. June 2018: Quarterly Network Vulnerability Scan to locate potential gaps in our network.
c. October 2017: Terminal Server Assessment: Removal of offsite access to District's Terminal Server. Disabling this feature will close the Remote Desktop Protocol for public access.
d. August 2016: Technology Infrastructure and Cyber-security Audit. Performed by GV/WFL BOCES and examined all servers, access, network, users, and services.

Audit Committee Chairperson: _____ 10/18/18
Bill Reigel Date

Administrator of Business and Operations: _____ 10-19-18
James Bruni Date