Article 27 GENERAL WORKING CONDITIONS

§ 27.1 Electronic Security Systems

The purpose of this section is to identify parameters for the use of electronic security systems that effectively address SEIU and the District's mutual interest in fostering a safe workplace while respecting and protecting the privacy of unit members. For purposes of this section, electronic security systems shall mean any electronically based technology that enables identification of the location and/or actions of specific persons at specific times. SEIU and the District agree to abide by the rules applicable to any form of surveillance in order to maintain a safe workplace and protect the unit members from all forms of malignant and invasive surveillance, regardless of the technology employed. SEIU and the District further agree to negotiate the terms implicated by the utilization of specific new technologies.

§ 27.1.1 Approved Purposes: The following are the sole approved purposes for the use of electronic security systems.

A. Protecting life and property.

B. Assisting in the investigation of a violation of law.

§ 27.1.2 Limitations on Placement of Electronic Security Systems

A. Security Camera Notification: The District shall reasonably locate clear signage providing notice that an area is monitored by a security camera.

B. Prohibition of Location: Electronic security systems shall neither be placed in, nor directed into, classrooms, conference rooms, restrooms, break rooms, other areas where unit members have a reasonable expectation of privacy, offices or where unit members regularly engage in professional duties except in the cases of overriding security concerns such as heightened general safety, cash handling, prescription drug storage, equipment storage, and high risk vandalism targets.

C. Changes to Locations Monitored by Electronic Security Systems: The District shall provide SEIU with a listing of the current locations monitored by electronic security systems. The District shall provide SEIU with written notice of any proposed change in locations monitored by security cameras or key-card-enabled door locks no less than thirty (30) business days in advance of making the proposed change. SEIU may, within twenty (20) business days of receiving such notice, demand to meet and confer with the District if it believes the proposed change violates this section or requires further impacts bargaining prior to implementation. Within ten (10) business days after the meet and confer process is completed, the District shall provide SEIU with written notice whether it intends to proceed with the proposed change. SEIU shall not file a grievance or other action asserting violation of this Article by the proposed change without first utilizing the meet and confer process afforded by this subsection. The District shall not proceed with the proposed change under this subsection during the meet and confer and/or grievance process.

D. Limits on Technology: Monitoring technologies used by District electronic security systems are limited to video security cameras and key-card-enabled door locks. Storage and/or analysis by a third party of any portion of the data obtained by District electronic security systems is prohibited. The use of facial recognition technology is prohibited.

Article 27 GENERAL WORKING CONDITIONS (Continued)

§ 27.1 Electronic Security Systems: (Continued)

§ 27.1.3 Limitations on Access to Data: Consistent with the approved purposes set forth in 27.1.1, data recorded by electronic security systems shall be accessed only under the following circumstances:

A. The District, through its Chief of Police (or designee), has probable cause that a violation of law has occurred and that access to the data would assist in the formal investigation.

B. Subject to a lawful subpoena, judicial order, or other legal obligation to produce the data to a third party.

C. As a result of an insurance investigation.

§ 27.1.4 Limitations on District Use of Data Accessed from Electronic Security Systems

A. Prohibition of Use for Reviewing and Evaluating Members' Performance. Data gathered from electronic security systems shall not be used to monitor unit members' attendance, work or work habits, nor shall such information be used in any part of the evaluation process.

B. Limited, Permissible Use for Disciplinary Purposes. Data accessed from an electronic security system shall not be used as evidence in a disciplinary action against a unit member, unless that action specifically involves a violation of law.

§ 27.1.5 Authorized Access: When one or more of the circumstances described in 27.1.3 has prompted a request for data from an electronic security system to be examined or disclosed, the following shall apply:

A. Authorization: Except for when required by law or in emergencies, access to data must be authorized in advance and in writing by the President or appropriate Vice President. The President or appropriate Vice President shall ensure that the request to access data complies with this Article.

B. Required by Law: When the District receives a search warrant, subpoena or other legally required request of electronic security system data, the data may be preserved immediately without authorization, but appropriate authorization for access must then be sought as soon as legally permissible.

C. Emergencies: In emergencies, the least perusal of data and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay. Emergencies are defined as when time is of the essence and there is a high probability that delaying action would almost certainly result in significant bodily harm, significant property loss, damage to the District or its assets, or loss of significant evidence of one or more alleged violations of law.

Article 27 GENERAL WORKING CONDITIONS (Continued)

§ 27.1 Electronic Security Systems: (Continued)

§ 27.1.5 Authorized Access (Continued)

D. District Police: This Article does not preclude the District Police department from accessing data in an investigation into a possible criminal violation of law.

E. Retention: Electronic security system data shall be retained for a period of no more than ninety (90) calendar days from the time of recording, unless the data is accessed within that period for an approved purpose consistent with this Article, in which case the data shall be retained as long as required by applicable law.

This page intentionally left blank.