NEW YORK CITY IDENTITY CARD (IDNYC) PROGRAM DATABASE SECURITY

TO: Martha Calhoun, General Counsel
Kathleen Carlson, Chief External Affairs Officer
Saratu Ghartey, Chief Program Accountability Officer
Matthew Brune, Chief Operating Officer
Jennifer Tavis, Executive Director, IDNYC Program
Lauren Friedland, Privacy Officer
Jon Miller, Chief Information Security Officer
All IDNYC Program Staff

CC: Nisha Agarwal, Commissioner, Mayor's Office of Immigrant Affairs
Mindy Tarlow, Director, Mayor's Office of Operations
Jennifer Yeaw, Chief of Staff, HRA
Jordan Dressler, Senior Advisor for Strategic Initiatives, HRA

FROM: Steven Banks, Commissioner
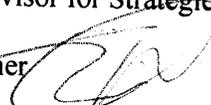
I.   INTRODUCTION

Pursuant to New York City Administrative Code Section 3-115 and the Mayor's Executive Order No. 6 of 2014, the New York City Human Resources Administration (HRA) is designated as the administering agency of the New York City Identity Card (IDNYC) Program. HRA and the IDNYC program are committed to protecting the privacy of IDNYC applicants' data through data security protocols designed to minimize the risk of unauthorized use and disclosure of applicants' and cardholders' personal information.

These protocols will apply to all of applicants' and cardholders' personally identifiable information, including but not limited to: name; address; scanned copies of identification and residence documents submitted for the card application; applicant photographs taken for the card; image templates derived from such photos; and any other information that may be used on its own or with other information to identify a person.

II.   DATA STORAGE

IDNYC applicant data will be stored in accordance with the New York City Department of Information Technology & Telecommunication (DoITT) Citywide Information Security Program and its requirements for the handling of confidential information.

These requirements are publicly available on DoITTs website: http://www.nyc.gov/html/doitt/html/business/security.shtml. Accordingly, IDNYC applicant data will only be stored on the IDNYC Program's own encrypted computers and servers. All such data will be erased from local computers once sent to the server. All transmissions of such data will be encrypted.

III.   DATABASE ACCESS

In accordance with the City's Identity Management Security Policy which requires that all access to City systems be authorized and based on individual identification and authentication, only HRA staff directly involved in the administration of the program, who have been trained and have been authorized by the Executive Director of the IDNYC Program or his/her designee or the General Counsel or his/her designee, will have access to the IDNYC program's databases. Moreover, HRA staff will have the lowest-level of access necessary to perform their jobs. Access to the databases and servers will be tracked through audit logs.

For information concerning the handling of third party requests for data contained in the IDNYC databases, please see the Commissioner's Executive Order No. 735 entitled "Handling of Third Party Requests for New York City Identity Card (IDNYC) Applicant and Cardholder Information."

IV.   ACTIONS TO BE TAKEN IN THE EVENT OF A DATA SECURITY INCIDENT

Any person who becomes aware of any data security incident involving data collected in connection with the IDNYC Program shall immediately report the incident to HRA's General Counsel and the HRA Privacy Officer so that HRA's Office of Legal Affairs may immediately commence an investigation to determine if there was an unauthorized disclosure of applicants' or cardholders' personally identifiable information and if so, the scope of any such disclosure. The Office of Legal Affairs will also establish an appropriate corrective action plan and take steps to mitigate any harm caused by the disclosure.

In the event of a data breach involving personally identifiable information of IDNYC applicants or cardholders, HRA shall provide notification to the affected individuals within a reasonable amount of time, but no later than 60 calendar days after the discovery of the breach or earlier if so required by law, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. Notification shall be in a format prescribed by the HRA Privacy Officer and shall meet the breach notification requirements of applicable local, state and federal law.

The improper use or disclosure of IDNYC data may result in disciplinary action as deemed appropriate by HRA, and a referral of the matter to the Office of the New York City Inspector General for potential prosecution.

Classification 1

Effective: Immediately