1. Privacy Policy Summary

We are committed to protecting user privacy with Sensor Andrew.

Please be assured that all Sensor Andrew research projects are in compliance with Carnegie Mellon's Institutional Review Board (IRB) procedures. No individual components of the Sensor Andrew research projects will begin collecting data until IRB clearance has been approved for that component.

Additionally, Sensor Andrew will not collect information that is associated with any individual person (or persons), unless specific opt-in procedures are implemented and clearly communicated prior to activation. In most cases, Sensor Andrew is sensing the physical infrastructure and environment and not directly sensing people or persons.

We believe it is important that you understand how we treat the information you may provide to us, or that we collect as a part of project. Unless specifically stated otherwise, the information you provide is never shared with anyone other than Sensor Andrew employees, faculty or authorized contractors. The list of these Sensor Andrew participants can be found at the following link:
http://www.ices.cmu.edu/censcir/faculty.html

If you have ANY questions or concerns regarding privacy and Sensor Andrew, please contact us at 412-268-8859.

2. Sensor Andrew Application Privacy Sensitivity Tiers

At Sensor Andrew, we recognize that some of the Sensor Andrew applications are more sensitive to privacy concerns than others. Therefore, we have divided this policy into two broad “tiers” of Sensor Andrew applications. The “privacy tier level” and associated policies will be clearly marked on the Sensor Andrew website for each Sensor Andrew application.

2.1 Tier 1 Privacy Applications (standard privacy applications)

In most cases, Sensor Andrew applications are sensing the physical infrastructure and environment and not people or persons. These projects will be called “Tier 1 Privacy Applications” in this Policy. Tier 1 projects cannot directly sense people within infrastructure, but only the condition or usage data of the infrastructure itself. Therefore, privacy concerns are limited to what can be inferred indirectly from data about the infrastructure and not from the occupants themselves.

2.2 Tier 2 Privacy Applications (sensitive privacy applications)

A small number of Sensor Andrew applications require the sensing of people, and all of these projects will require the individuals affected by this application to “opt-in” prior to the activation of their participation in the application. These Sensor Andrew applications will be referred to as “Tier 2 Privacy Applications” and will require a higher level of privacy control and monitoring to ensure that Sensor Andrew is maintaining the high level of respect for individual privacy.
No data about any individual will be collected without prior opt-in permission from that individual, and that individual retains the right to change his/her mind at any time. In the event of an individual withdraws his consent for being monitored, all previously recorded data pertaining to this person will be destroyed.

Additionally, all Tier 2 applications will be required to comply with all Tier 1 Privacy rules as outlined in this document AT A MINIMUM, and are required to maintain any additional privacy policy addendums that may be relevant to their own applications. All privacy policies applicable to Tier 2 applications must be clearly posted on their primary Sensor Andrew websites. By definition, all Tier 2 applications are required to maintain a purely opt-in operation.

3. Collection Purpose, Use Limitation and Data Retention

Sensor Andrew sensors will always be clearly marked with the Sensor Andrew logo and information on how to find out more about what they are collecting, why, the individual sensor data-retention rates and other sensor information via a web-link or telephone number. In cases when the unit is out of sight or reach a label must be placed within 100 meters from the device.

Additionally, information on all active Sensor Andrew sensors, their purpose, parameters, data collection rates and data retention rates will be posted on the main Sensor Andrew website. Each project associated with Sensor Andrew will have a section on their website outlining what sensor data they are collecting and why they are using this data.

Also, Sensor Andrew researchers responsible for individual sensors will make a consistent effort to communicate with the community in which the sensors are to be placed prior to their installation, e.g., via a memo and/or sign, a poster placed at a visible location with contact information. The memo will include information about what the sensors are collecting, why, the individual sensor data-retention rates and other methodologies.

Data will be collected at a resolution and quality that meets the needs of the individual Sensor Andrew applications researcher, but will not exceed these requirements (i.e., the sensors will not collect more data than necessary for the intended purpose of the research). This data will be anonimized according to standard procedures, unless the goal of the application precludes this and the individuals have opted-in.

Except in the case of opt-in applications, no information directly linking an individual with data will be provided to internal or external parties. Data linking personal information with anonymous information will be stored in a secure location where only authorized administrators will have access for troubleshooting and maintenance purposes. However, we may disclose this information if required by law, subpoena, court order or other legal process.

Approved research groups will be allowed access to anonymous information. Data not linked to individuals such as sensor data collected in public areas will be available to all users. Software with applicable user interfaces must have a mechanism for displaying what type of information may be stored or shared with other devices. The data generated by any of the projects will remain anonymous for public presentation.

No hidden sensors or databases will be maintained.
4. **Reasonable Security**

All Sensor Andrew applications, databases, and wireless networks will provide reasonable security and maintain patch levels, etc. as needed understanding that Sensor Andrew is a research project. By its nature as a research project, Sensor Andrew cannot provide the same level of security as a commercial product or project.

5. **Openness and Transparency**

The Sensor Andrew website will maintain clear descriptions of all Sensor Andrew data collection activities and sensor locations. Sensor Andrew and its Principal Investigators will endeavor to be as transparent and timely as possible about any changes in data collection, retention and storage activities.

No hidden databases or sensors will be installed or maintained.

6. **Accessing and Updating Personal Information**

When you use a Sensor Andrew application, we make good faith efforts to provide you with access to your personal information and either to correct this data if it is inaccurate or to delete such data at your request if it is not otherwise required to be retained by law or for legitimate research purposes. We ask individual users to identify themselves and the information requested to be accessed, corrected or removed before processing such requests, and we may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort, jeopardize the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes), or for which access is not otherwise required. Some of our services have different procedures to access, correct or delete users' personal information. We provide the details for these procedures in the specific privacy notices or FAQs for these applications.

7. **Individual Participation**

As noted in Section 2 above, a small number of Sensor Andrew applications require the sensing of people, and all of these projects will require the individuals affected by this application to “opt-in” prior to the activation of the application. These Sensor Andrew applications are referred to as “Tier 2 Privacy Applications” and will require a higher level of privacy control and monitoring to ensure that Sensor Andrew is maintaining the high level of respect for individual privacy.

No data about any individual will be collected without prior opt-in permission from that individual, and that individual retains the right to change his/her mind at any time.

Additionally, any Tier 1 application that “indirectly” senses infrastructure parameters in a privately occupied space (such as an individual office) will have to obtain opt-in approval from each individual that may be affected.

We may share with third parties certain pieces of aggregated non-personal information such as sensor data in public spaces. Such information does not identify you individually.
8. Accountability and Privacy Compliance Audits

Sensor Andrew will appoint a Chief Privacy Officer (Matthew Sanfilippo is acting CPO for the launch of the project) who will perform annual audits of all Sensor Andrew project components to ensure compliance with this privacy policy. Additionally, the Privacy Officer will perform occasional spot checks for compliance and will act as a privacy resource for all Sensor Andrew investigators.

ALL Sensor Andrew Project Participants must sign a copy of this policy and submit it to the Sensor Andrew Privacy Officer indicating their understanding of (and commitment to) this policy prior to activation of their Sensor Andrew application.

Additionally, all Sensor Andrew principal investigators must complete and return the attached checklist form to the Sensor Andrew Privacy Officer. This form must be completed in place prior to activation of the individual application.

9. Email and Newsletters

If you no longer wish to receive our newsletters and communications from Sensor Andrew, you may opt-out of receiving them by contacting 412-268-8859.

10. Sales or Trading of Data

Sensor Andrew does not sell or trade your personal information.

11. Changes to This Privacy Statement

We reserve the right to modify this privacy statement at any time, so please review it frequently. If we decide to change our privacy policy, we will post those changes to this privacy statement, the homepage, and other places we deem appropriate so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it.

12. Contact Us

If you have ANY questions or concerns regarding privacy and Sensor Andrew, please contact Matt Sanfilippo at 412-268-8859.

By signing below, the signer is indicating that they understand this Privacy Policy and will work to ensure that their research complies with the Universities IRB policies as well as this Privacy Policy.

Sign Here ____________________________
Print Name___________________________
Date_________________________________
Sensor Andrew Application Checklist

This Checklist must be completed and submitted to the Sensor Andrew Privacy Officer prior to installation of Sensors

(Please initial next to each item as it is completed)

1. Sign and return the Privacy Policy to the Sensor Andrew Privacy Officer

Initial here when complete: ____________ Date: ____________

2. Discuss your Sensor Andrew project with the Sensor Andrew Privacy Officer to determine if your application is a Tier 1 or a Tier 2 application.

Initial here when complete: ____________ Date: ____________

3. Obtain IRB approval or determine that IRB approval is not needed. Please see http://www.cmu.edu/osp/compliance/human-subjects.html for more detail on how to obtain an IRB and to determine if one is needed.

Initial here when complete: ____________ Date: ____________

4. Clearly label all Sensors, Gateways and other equipment that are required for your application with stickers that show the Sensor Andrew logo and a web link and/or phone number where people can obtain information on the type, purpose, individual sensor data-retention rates and other information.

Initial here when complete: ____________ Date: ____________

5. Provide detailed information on your Sensor Andrew application, sensor types, gateway types, data collection purposes, individual sensor data-retention rates and other information in electronic format to the Sensor Andrew website manager for inclusion in the public website and privacy policy.

Initial here when complete: ____________ Date: ____________

6. If your application is a Tier 2 privacy application, develop an opt-in procedure for your application and get it approved by the Sensor Andrew Privacy Officer.

Initial here when complete: ____________ Date: ____________
7. Develop and widely circulate a memo and/or sign that communicates with the community in which the sensors are to be placed prior to their installation. The memo will include information about what the sensors are collecting, why, the individual sensor data-retention rates and other methodologies.

Initial here when complete: _____________ Date: _____________

8. Develop procedures that will provide your Sensor Andrew applications, databases, and network with reasonable security and maintain patch levels, etc as needed understanding that Sensor Andrew is a research project. By its nature as a research project, we understand Sensor Andrew cannot provide the same level of security as a commercial product or project.

Initial here when complete: _____________ Date: _____________

By signing below, the signer is indicating that they have completed all of the above items for their Sensor Andrew application

Sign Here ___________________________________
Print Name_________________________________
Sensor Andrew Application Name_________________
Privacy Tier Level___________________________
Date_____________________________________