

## Information Security Policy

At Icomera, we value the individual's integrity. In order to provide a service to passengers for our customers, on board vehicles across the world, we do need to keep some data about the individuals. The data we store include the MAC address and IP address of the device used for the connection and the time the connection was established. We do not encourage our customers to collect any further information about their passengers besides what is necessary for them to make it a safe and pleasant journey.

Information Security is a core fundamental element which supports and underpins everything we do. We understand that Information Security is a continually evolving area which we are determined to invest in to ensure we maintain and enhance our forefront position.

We use globally recognised Information Security standards to provide evidence that our activities conform to current global best practices and regulations.

We train our staff in Information Security related matters and in Security Awareness. We also work towards information security being a state of mind for all departments' staff members, and in the tasks associated with their roles.

We use the CIA triad to judge Information Security risks and mitigating actions:

- Confidentiality -The information shall only be seen by those who have the right to see it
- Integrity - You shall be able to trust the information given is correct
- Availability -The information shall be available to those who have the right to access it when they need it and when it is relevant for them to access it

Although we have little control over major incidents outside of the Icomera network, the Icomera Information Security Office monitors external information and intelligence sources for new emerging threats, to help minimise the impact on the global estate.

## Document Information

<b>Document Classification</b>	Public
<b>Document Type</b>	Policy
<b>Author</b>	Information Security Office
<b>Approved By</b>	Management Team
<b>Version</b>	4.3
<b>Approved Date</b>	2021-02-26
<b>Last Review Date</b>	2021-02-18

## Revision History

<b>Date</b>	<b>Version</b>	<b>Comment</b>
<b>2017-12-06</b>	1.0	Created
<b>2018-02-06</b>	2.0	Comments and changes based on feedback from Jörgen C
<b>2018-02-20</b>	3.0	Approved version by Management Team
<b>2018-03-12</b>	4.0	Reworked version (final approval pending from management team on 26 April 2018)
<b>2018-04-18</b>	4.1	Minor additions after comments from auditor
<b>2018-04-26</b>	4.1	The version approved on management team meeting
<b>2019-01-02</b>	4.2	Review by Security Office, word change to match new terminology of major security incidents instead of breaches
<b>2021-02-18</b>	4.3	Rephrased to clearly state our commitments and how we work towards our security goals.
<b>2021-02-26</b>	4.3	The version approved on management team meeting