LINXCAD

Privacy Policy

What we collect, why, and who sees it.

> **Draft.** This text has not yet been reviewed by a lawyer and is not in force. Items in [square brackets] are still to be filled in.

Effective date: [EFFECTIVE DATE]

This Privacy Policy explains how [BUSINESS LEGAL NAME], doing business as LinxCAD (**LinxCAD**, **we**) handles information on the linxcad.com website and in the LinxCAD software service (the **Service**).

1. Two kinds of information, two roles

- **Website and sales information** (people who visit linxcad.com, ask for a demo, or contact us): we decide how it is used and are responsible for it.
- **Customer Data** (everything a customer's employees and administrators put into the Service, such as reports, calls, photos, logs, location and user accounts): the customer decides what is recorded and why. We process it on the customer's behalf, under the customer agreement. If you work for a customer or appear in its records, the customer is who to ask about your information (see section 8).

2. What we collect

- **Website and sales:** what you tell us when you email or ask for a demo through the form on our website (your name, company, email address, your line of work, your message, and a phone number if you give one). The form also keeps a scrambled version of your IP address, which we use only to slow down spam and cannot turn back into your address. We email these details to our staff so we can reply, and keep them in our own list of requests. Our hosting also records basic technical data, such as IP address and pages requested.
- **Accessibility choices:** if you use the accessibility button on our website, your choices (text size, contrast and so on) are saved in your own browser's local storage so they carry from page to page. They stay on your device and are not sent to us.
- **Account data in the Service:** name, username, role, email, phone, employee ID or callsign, and a password stored only as a salted hash. Administrators and platform staff using two-factor sign-in also have an authenticator secret stored encrypted.

- **Billing information** (customers who subscribe): the organization's name, the owner's name and email, billing address, tax ID if given, the plan, and whether payments are up to date. Card details are entered on Stripe's pages and held by Stripe.
- **Device data:** a device identifier, a label and model name, and a device key used to prove the device is approved.
- **Location:** when the phone app is signed in it shares the device's location with the customer's company so dispatch and supervisors can see where officers are. Location history is deleted after 7 days. Location is also recorded with patrol checkpoint scans, and, if the customer uses the on-site access feature, sent with requests so the server can check the person is near one of the company's locations; that check is not stored. The phone shows a notification while location sharing is running.
- **Customer content:** calls, reports and their narratives, activity log entries, notes, messages, patrol records, shift and timecard records, photos and signatures, records of people and vehicles entered by the customer (which can include names, birth dates, addresses, phone numbers, ID numbers and descriptions of members of the public), and invoices and customer lists if those features are used.
- **Security and audit records:** sign-in attempts and administrative actions (who did what and when).
- We do **not** use advertising identifiers, advertising networks or third-party analytics in the mobile app.

3. How we use it

- To provide, secure, support and improve the Service for customers.
- To respond to people who contact us and to send service messages (invitations, notifications the customer has turned on, invoices, security notices).
- To keep records, prevent abuse and meet legal obligations.
- We do not sell personal information and do not use Customer Data to advertise or to train models.

4. Who we share it with

We share information only with service providers who help us run the Service, and only as needed:

- **Hosting and infrastructure** where the Service runs [CONFIRM: provider and location].
- **File storage:** photos, signatures and logos are stored in a private Cloudflare R2 bucket, encrypted at rest by Cloudflare.
- **Email delivery** for the messages the Service sends.
- **Map and address services:** map tiles (Esri, CARTO) and address search (OpenStreetMap Nominatim, and others configured), which receive the viewer's IP address and the area viewed or the address searched.

- **Software updates** through GitHub, which receives the device's IP address and app version.
- **Payment processing** through Stripe, which collects the payment details, billing address and tax ID when a customer subscribes, works out sales tax, and keeps the record that the customer agreed to our terms. We do not see full card numbers [CONFIRM when enabled].

We may also disclose information if the law requires it, to protect people's safety or our rights, or in a business sale (with the same protections). Within a customer, its administrators and supervisors can see its data as the customer's settings allow. LinxCAD staff see Customer Data only as the customer allows (see the agreement).

5. How long we keep it

- Location history: 7 days. Current location: removed when the person's shift ends or they sign out.
- Photos: as long as the customer's retention setting says (30 days, 90 days, 1 year or forever).
- Reports, the activity log and other records: until the customer deletes them or the agreement ends, then deleted within the period in the agreement.
- Website and sales messages, including demo requests: as long as needed to deal with your request and for our records. Ask us and we will delete yours.
- Sign-in sessions: up to 30 days on the apps (and ended earlier when the app closes or sits idle) and 8 hours on the web portals.

6. Security

We protect information with separation of each customer's data, hashed passwords, two-factor sign-in for administrators, approved devices, role-based access, encrypted connections and activity records. No method is perfectly secure, and we cannot guarantee absolute security. If we learn of a security incident affecting customer data we will notify the customer as the agreement describes.

7. Health information

The Service is built for security operations and is not designed to store protected health information. Customers are told not to enter patient names or medical details beyond what an incident report needs, and the Service includes ways to leave names out. We do not act as a HIPAA business associate unless a separate written agreement says so.

8. Your choices and rights

If you are an employee or a member of the public in a customer's records: contact that organization to ask to see, correct or delete information about you. If you contact us, we will pass the request to the customer and help it respond.

If you contacted us through the website: email privacy@linxcad.com to see, correct or delete what we hold. Depending on where you live, you may have more rights (for example to know what we collect, delete it, or opt out of its sale or sharing). We do not sell or share personal information for advertising. We will not treat you differently for using your rights.

9. Employees and location

Customers decide whether to use location, shift and timecard features and are responsible for telling their employees and obtaining any consent the law requires. Employees with questions should ask their employer.

10. Children

The Service is for businesses and their workers and is not directed to anyone under 18.

11. Where information is processed

The Service is operated in the United States [CONFIRM] and information is processed there.

12. Changes and contact

We may update this policy and will post the new date. For a material change affecting customers we will give notice as the agreement says. Questions: privacy@linxcad.com, [BUSINESS LEGAL NAME], [MAILING ADDRESS].