The Executive Digital Hygiene Checklist (2025 Edition)

By Dinez Carnay, Founder of Dinez Executive Chauffeurs

A Note from the Founder: *"In the executive world, discretion isn't a luxury—it's an operational necessity. We built Dinez on a promise of absolute physical security and privacy. This blog post extends that promise to your digital perimeter, because true risk mitigation requires securing both your journey and your data."*

5 Steps to Mitigate Surveillance Risk on Work-Managed Devices

Why You Need This Audit Now

> The recent Google update enabling **RCS Archival** on employer-managed Android devices means text messages (SMS and RCS) are now subject to corporate review, bypassing the perceived security of end-to-end encryption. **Privacy on a company phone is now an operational assumption, not a guarantee.** This audit provides an immediate path to segregation and risk mitigation on business work phone and travel.

Phase I: The New Threat Landscape

The Core Problem: Decrypted Data at Rest

The widespread misunderstanding of End-to-End Encryption (E2EE) is driving this new crisis. E2EE secures messages *in transit* (while they are being sent), but once the message lands on a device managed by your organization, the decrypted content is considered **data at rest**. New compliance tools leverage this access point to archive messages before they are viewed.

This affects any employee using a company-issued **Android device**, especially **Google Pixel models**, under a formal Mobile Device Management (MDM) framework.

For detailed regulatory context on data logging requirements, refer to the Forbes report on the Google RCS Archival update and corporate liability (Source: *Executive Tech Compliance Review 2025*).

Phase II: The 5-Point Executive Audit

This audit is designed to deliver **immediate digital risk segregation** and ensure your communications are compliant and secure.

Action Point	Digital Hygiene Protocol	Risk Mitigation Outcome
1. The Segregation Mandate	Implement the "Two-Device" Policy. Use the work phone exclusively for sanctioned corporate tools. Move ALL personal communication (banking,	Eliminates the single point of failure and protects personal liability against legal discovery.

	personal contacts, non-work chats) to a dedicated, unmanaged private device.	
2. Device Management Verification	Access your device settings and locate the "Security" or "Device Administrators" menu. Look for the "Managed by your organization" notification or any unfamiliar archival apps (e.g., Smarsh, Celltrust).	Confirms the exact level of control your employer has over the hardware and prevents clandestine monitoring.
3. RCS and SMS Protocol Review	Disable RCS (Chat Features) within the Google Messages app on the work device. Assume all remaining SMS (standard text) is logged via carrier or compliance software. Only use approved enterprise tools for all business communications.	Stops the automatic archival of Rich Communication Services (RCS) messages at the device level.
4. High-Security Communication Pivot	For any sensitive, personal conversations required while traveling, transition immediately to high-security, third-party encrypted applications (e.g., Signal). **Do not install these apps on the work-managed device.**	Ensures conversations stay truly E2EE, where the keys remain only on unmanaged private devices.
5. Policy and Consent Check	Review your current Employee Handbook, IT Use Policy, and any signed MDM consent forms. Note the specific language regarding **"Retention"** and	Establishes your compliance boundaries and legal standing in the event of an HR or compliance inquiry.

	"Monitoring of Personal Data."	

FAQs:

High-value executives often have immediate, pressing questions. We address the most common fears here:

Q: Does this Google RCS Archival affect my personal, unmanaged Android phone?

A: No. This feature is specifically enabled by corporate IT departments using Mobile Device Management (MDM) software on company-issued or "fully managed" devices. Your personal, private phone remains protected by E2EE.

Q: Can my employer access messages I edit or delete?

A: Yes, likely. The new archival tools often capture the message event *at the time of sending*, including the original, unedited text. Deleting the message from your device screen typically only removes the local copy, not the version logged by the archival server for compliance purposes.

Q: Why are companies doing this now?

A: This is primarily driven by regulatory pressure (e.g., SEC, FINRA) that requires all business communication—including texts—to be logged and auditable. Google's update simply provides a reliable, supported mechanism for companies to achieve this compliance standard on their fleet of Android devices.

Trust and Risk Mitigation

At Dinez Executive Chauffeurs, we understand that executive travel is about more than just transport; it's about **seamless operations and risk mitigation.**

In a world where digital boundaries are dissolving, your need for reliable, secure, and private service is paramount. Just as we ensure your physical journey is monitored, secure, and discreet, we urge you to treat your digital footprint with the same level of professional scrutiny.

Take the 5-point audit today. For unparalleled security and discretion on the road, trust Dinez—your partner in executive risk management.

Contact:

Dinez Taxis and Airport Transfers

151 Grosvenor Road, Aldershot, GU11 3EF | 01252 265363