MARLUC

CASE STUDY · MARLUC SYNOPSIS

Samsung ChatGPT leak and ban

IMPLEMENTED 2023–2026 · MANUFACTURING AND INDUSTRIAL · SOUTH KOREA · BAND F · REVERSED

VERSION 1.0 · PUBLISHED 16 NOVEMBER 2026 · UPDATED 16 NOVEMBER 2026 · FACTS CHECKED 16 NOVEMBER 2026

Weeks after Samsung's chip division allowed staff to use ChatGPT in 2023, employees reportedly entered source code, test data and meeting notes into it. Samsung restricted and then banned generative AI tools; in 2026 it reintroduced external AI services through enterprise versions.

ABOUT THIS SYNOPSIS

This is MarLuc's summary and grading of publicly available sources, for information only. It is not investment, legal, financial or professional advice, and should not be relied on for any decision. Readers must validate it against the original sources and, where appropriate, challenge its conclusions.

Facts and figures are as reported by the sources listed below, which may be incomplete, self-reported or out of date. Check the original source before relying on any figure.

The impact band, proof marker and SEAM view are MarLuc's opinion. The organisation is not a MarLuc client and has not reviewed or endorsed this synopsis. Names and trademarks belong to their owners.

NOTICE WORDING LAST UPDATED 16 NOVEMBER 2026

AT A GLANCE

What went wrong: Weak oversight or controls.

AI used: Public generative AI chat assistant (ChatGPT) used by staff; later enterprise AI tools.

Implemented: 2023–2026. Grade: band F, Failure, Reversed.

Headline result, as reported: Three reported leaks of confidential data into ChatGPT within 20 days of permission in 2023, followed by a ban; external AI tools reintroduced through enterprise versions in 2026

1 · The case

The facts, as reported by the 5 sources listed at the end. Where a source is silent, the field says "Not reported".

Organisation

Samsung Electronics. South Korean electronics and semiconductor manufacturer. The 2023 incidents were reported in its Device Solutions (semiconductor) division; the 2026 reintroduction began in its Device Experience (DX) division, which makes phones, consumer electronics and appliances. Canvas block: 8. Governance and risk. Also 5. People and skills, 6. Data and technology.

Business challenge

The challenge. Not reported as a business problem. Engineers reportedly used ChatGPT to fix errors in source code, optimise test sequences and produce meeting minutes.

How it was addressed. Samsung's semiconductor business let its fab engineers use ChatGPT in early 2023, per Tom's Hardware's report of The Economist Korea. Within about 20 days, three incidents were reported: an employee entered source code from a proprietary program to fix errors, another entered test patterns for identifying defective chips, and a third submitted a converted meeting recording. Samsung warned staff that data entered into ChatGPT is stored on external servers and cannot be retrieved, and limited prompts to 1,024 bytes. In May 2023 an internal memo, reported by Bloomberg and confirmed by the company per The Register, banned tools such as ChatGPT and Bard on company devices. Samsung encouraged use of its in-house platform, Gauss. In June 2026 the DX division allowed ChatGPT, Gemini Enterprise and Claude; OpenAI then said ChatGPT Enterprise and Codex would reach all Samsung Electronics employees in Korea and all DX staff worldwide. [1] [2] [3] [4] [5]

Who implemented it

OpenAI (Model or cloud provider): Provider of ChatGPT in 2023 and of ChatGPT Enterprise and Codex in 2026.
In-house (In-house): Samsung Electronics: developed the in-house Gauss platform.
Google (Gemini Enterprise) and Anthropic (Claude) are also named as services the DX division allowed from June 2026.

Technology (SEAM pillar E)

SEAM types: T1 Chat assistants. Deployment: Vendor SaaS. Vendors and products: OpenAI, Google, Anthropic, ChatGPT, ChatGPT Enterprise, Codex, Gemini Enterprise, Claude, Samsung Gauss.

Where it was built in: In 2023, staff used the public ChatGPT service directly. From 2026, enterprise AI services are used across DX operations alongside Samsung's in-house Gauss platform, which is integrated with internal systems.

What changed

Before: semiconductor staff could use public ChatGPT. After the incidents: prompts were limited, then generative AI tools were banned on company devices in May 2023. In 2026: external tools returned through enterprise versions with access and data controls, alongside Gauss. [1] [2] [3] [4] [5]

Cost of failure

Not reported. The value of the data entered into ChatGPT, any disciplinary outcome and the cost of the ban are not reported. Samsung declined to confirm or deny the incidents, per Tom's Hardware.

What it saved

Not reported [1] [2] [3] [4] [5]

Governance and control

The incidents were followed by a warning to staff, a 1,024-byte prompt limit and, in May 2023, a ban on generative AI on company devices, per press reports. The 2026 rollout uses ChatGPT Enterprise, which OpenAI says includes data protection, user access and security controls. Accountable owner: Not reported.

S2 · Accountable owner · Not reported
Not reported.

A1 · Safe use · Missing (independent source shows it was absent)
Three incidents of confidential data being entered into ChatGPT were reported within about 20 days of permission, after which Samsung warned staff and limited prompt length. [2] [3]

A2 · Human in the loop · Not reported
Not reported.

A3 · Monitoring and assurance · Evidenced
The semiconductor business recorded three instances of ChatGPT use that led to data leaks, per Tom's Hardware's report of The Economist Korea. [2]

A4 · Vendor AI · Claimed
The 2026 rollout uses ChatGPT Enterprise, which OpenAI says includes data protection, user access and security management controls. [5]

A5 · Agent controls · Not reported
No agents described.

A6 · Standards and regulation · Not reported
Not reported.

What worked, what did not, what is unproven

WORKED

– Not reported for the 2023 permission.

– The 2026 reintroduction gives staff a choice of enterprise tools alongside the in-house Gauss platform, by Samsung's account.

DID NOT

– Staff reportedly entered source code, chip test patterns and meeting content into a public AI service within about 20 days of permission, per Tom's Hardware.

– Data entered into ChatGPT is stored on external servers and cannot be retrieved, Samsung warned staff, per Tom's Hardware.

– The permission was withdrawn: generative AI tools were banned on company devices in May 2023.

UNPROVEN

– Whether any leaked data was misused: Not reported.

– Whether the enterprise controls introduced in 2026 prevent similar exposure.

– When the Device Solutions division will introduce external AI services; the Korea Times reported in June 2026 that no schedule had been finalised.

Timeline

Apr 2023 Press reports three leaks of confidential data within about 20 days of the semiconductor

Apr 2023 Prompts limited to 1,024 bytes after the incidents, per press reports [3]

May 2023 Internal memo bans generative AI tools such as ChatGPT on company devices, per Bloomberg [1]

Jun 2026 DX division allows ChatGPT, Gemini Enterprise and Claude; in-house Gauss stays in use [4]

Jun 2026 ChatGPT Enterprise and Codex extended to all employees in Korea and all DX employees worldwide, per OpenAI [5]

2 · Grade and SEAM assessment

MarLuc's opinion, made on the evidence above. How cases are graded: marluc.co.uk/case-studies/how-we-rate

Level of change and impact

Claimed: Not applicable. Grade: F, Failure. Proof: Reversed. Level of change: Not graded.

No level assessed: band F, a staff permission to use a public AI tool that was withdrawn after reported data exposure. The case shows how quickly informal use can expose confidential engineering data.

Band F: a live permission to use a public AI tool was withdrawn after confidential data was reportedly exposed. The 2026 reintroduction through enterprise versions shows the company returning to external tools under different controls.

The SEAM view and lessons learnt

The failure sat at the join between people and data: a public tool was opened to engineers before rules and controls on what could be entered were in place. Samsung first restricted and banned the tool, then returned to external AI through enterprise versions with access controls. For any manufacturer with valuable designs or process data, the order matters: set data rules and choose enterprise terms before opening the door.

1. Set rules on what data may be entered before allowing public AI tools.
2. Prefer enterprise versions with data controls for engineering work.
3. Train staff on data handling before granting access.

Evidence

Score 2 of 4. Independent press: reports based on The Economist Korea and Bloomberg; Samsung declined to confirm the leak details. The 2026 change is Samsung's own statement.

Evaluation method. Press reporting of internal incidents and an internal memo; company statement for the 2026 rollout.

Sources disagree. Tom's Hardware reports that the third employee prepared a presentation from a meeting recording; CFO Dive and The Register describe meeting minutes. Tom's Hardware reports test patterns for identifying defective chips; CFO Dive describes program code for identifying defective equipment.

3 · Original sources

Read these in full. To challenge a fact or a grade, use the contact form at marluc.co.uk or the link on https://marluc.co.uk/case-studies/samsung-chatgpt-leak-and-ban

[1] The Register: Samsung puts ChatGPT back in the box after 'code leak' (May 2023)
https://www.theregister.com/2023/05/02/samsung_generative_ai_ban/

[2] Tom's Hardware: Samsung fab workers leak confidential data to ChatGPT (April 2023)
https://www.tomshardware.com/news/samsung-fab-workers-leak-confidential-data-to-chatgpt

[3] CFO Dive: Samsung employees leaked corporate data in ChatGPT: report (April 2023)
https://www.cfodive.com/news/Samsung-Electronics-ChatGPT-leak-data-privacy/647309/

[4] The Korea Times: Samsung Electronics to introduce ChatGPT, Gemini, Claude in operations (June 2026)
https://www.koreatimes.co.kr/amp/business/tech-science/20260611/samsung-electronics-to-introduce-chatgpt-gemini-claude-in-operations

[5] AI News: Samsung opens ChatGPT Enterprise and Codex access after AI restrictions (June 2026)
https://www.artificialintelligence-news.com/news/samsung-chatgpt-enterprise-codex-employee-ai-use/

Samsung Electronics website: https://www.samsung.com

Version 1.0 · Published 16 November 2026 · Updated 16 November 2026 · Facts checked against sources 16 November 2026 · Downloaded 26 November 2026. This PDF may be out of date: the latest version, and a way to report an error or a better source, is at https://marluc.co.uk/case-studies/samsung-chatgpt-leak-and-ban

VERSION HISTORY

v1.0 16 November 2026 First published