November 25, 2026

Company name: **Osaki Electric Co., Ltd.**
Name of representative: Yoshihide Watanabe,
Chairman and CEO
(Securities code: 6644; TSE Prime Market)
Inquiries: Ryuichi Ueno,
Director and Senior Managing Executive Officer,
Head of Group Strategy Division
(Telephone: +81-3-6694-7140)

Notice Concerning Suspension of Production Due to Ransomware Cyberattack (Third Report)

Outlook for Resumption of Operations

Osaki Electric Co., Ltd. ("the Company") hereby announces, as reported in the "Notice Concerning Suspension of Production Due to Ransomware Cyberattack (First Report)" dated November 18, 2026 and the Second Report dated November 20, 2026, that it has confirmed that its systems were subjected to a ransomware cyberattack on November 17, 2026. The Company sincerely apologizes once again for the significant inconvenience and concern caused to its customers and all other parties concerned.

Since then, the Company, in cooperation with external specialists, has been verifying that the route of intrusion has been blocked and confirming the safety of its systems and devices. As the Company now expects to resume operations beginning with those areas where safety has been confirmed, the Company provides an update on the situation as of Wednesday, November 25, 2026, as outlined below.

Please note that the investigation is ongoing, and the information provided herein may change depending on the findings of further investigations. Should any changes occur, the Company will promptly announce them through its official website and other means.

1. Summary of This Report

(1) Resumption of operations: Having blocked the route of intrusion, the Company plans to resume production in stages from Friday, November 27, 2026, beginning with those areas where safety has been confirmed. The timing of the resumption of shipments for existing orders and of the acceptance of new orders will be announced separately from production. For details, please refer to "3. Outlook for Resumption of Operations."

(2) Information leakage: The Company has confirmed that data was transmitted from its internal systems to an external destination. The content and scope of the transmitted information are currently under investigation.

(3) Products and production equipment: The Company has confirmed that this incident did not affect its production equipment. No impact on the operation of products and services currently in use by customers has been identified to date.

(4) Group companies: Unauthorized access to Osaki Electric Systems Co., Ltd. has been confirmed. The impact on group companies on the same network is currently under investigation. For details, please refer to "6. Impact on Group Companies."

2. Status of Recurrence Prevention and Safety Verification

To prevent re-intrusion and re-encryption, the Company has implemented the following measures and is proceeding with safety verification.

Item	Measures implemented / verification status
Route of intrusion (VPN device)	The compromised device and the servers, etc. that may have been used to relay unauthorized access have been shut down and have not been restarted. External connections will be resumed after the safety of the connection method and authentication measures has been confirmed.
Authentication and accounts	The Company is verifying the status of password resets and the application of multi-factor authentication.
Servers (virtual and physical)	Within the scope verified to date, no evidence of tampering with servers or remaining encrypted files has been identified. Monitoring and protection are ongoing.
Data on file servers, etc.	Within the scope verified to date, no remaining encrypted files have been identified. The Company is verifying the safety of data, including whether any tampering has occurred, and will resume use of data as verification is completed.
Internal PCs	The Company is verifying the safety of devices. Devices on which unauthorized access has been confirmed have been isolated, and use will be resumed in stages for devices whose safety verification has been completed.
Web services and business systems / Portable PCs	To prevent unauthorized access via devices or credentials, the Company is resetting credentials and verifying access controls. Use will be resumed as verification is completed.
Production equipment	The production equipment network is in principle separated from the business network, and the Company has confirmed that this incident did not affect its production equipment.

Through the above measures, the Company considers that the risk of re-intrusion through the same route and of re-encryption of its internal systems has been reduced. Operations will be resumed only in those areas where safety has been confirmed. Use will continue to be restricted in areas where verification has not been completed, and monitoring will be strengthened after recovery.
The investigation into the information leakage will continue separately from decisions on the resumption of operations.

3. Outlook for Resumption of Operations

(1) Policy: Beginning with those areas where safety has been confirmed, the Company will switch in stages from manual handling to normal operations using its systems. After production resumes, shipments for existing orders will be made in stages once the conditions required for shipment have been confirmed. The switch to normal operation for new orders will proceed separately from shipments, after confirming the connection with customers' systems.

Item	Expected resumption / normalization	Remarks
Production (Saitama R&D and Manufacturing Center; Iwate Osaki Electric Co., Ltd.; Osaki Platech Co., Ltd.)	From Friday, November 27	Production will be resumed in stages using devices, systems and data whose safety has been confirmed.
Shipments for existing orders	From Tuesday, December 1	After production resumes, shipments will be resumed for products for which the conditions required for shipment have been confirmed. Delivery schedules will be communicated individually.
New orders (ordering/order acceptance and connection with customers' systems)	From Monday, December 7	For customers connected via system integration, resumption will proceed in stages for each customer as confirmation is completed.

(2) Response to customers: Delivery schedules for existing orders and system connections for the resumption of new orders will be communicated individually by the relevant business division or Purchasing Department of the Company.

(3) Note: The planned resumption dates are current estimates and may change depending on the progress of safety verification. Should any changes occur, the Company will promptly announce them through its official website and other means.

4. Information Leakage

(1) Facts identified: On November 19, 2026, the Company became aware that technical information believed to be stored in its systems had been posted on a website on the internet. Subsequent investigations have confirmed that, as a result of the unauthorized access, data had been transmitted from the Company's internal systems to an external cloud storage service.

(2) Status of investigation: As the verification of logs is taking time, the content and scope of the information transmitted externally remain under investigation.

(3) The Company's response: The Company is proceeding with procedures to request the provider of the service concerned to preserve, isolate and delete the data. The Company continues to consult with and report the incident to the police and other relevant authorities. The Company's policy is not to comply with the attacker's demands.

(4) Personal information and business partner information: Whether the information transmitted externally includes personal information is currently under investigation. The Company will take the necessary actions in accordance with applicable laws and regulations, including reporting the incident to the Personal Information Protection Commission and notifying the affected individuals. If the leaked information includes information managed under confidentiality agreements with business partners, the Company will contact the relevant business partners individually.

(5) Request: Please do not access or disseminate what is described as "technical information believed to be stored in the Company's systems." The Company cannot accept responsibility for any damage arising from access to the website concerned; please refrain from accessing it under any circumstances.
In addition, even if you come across what is described as "technical information believed to be stored in the Company's systems" on the internet, please do not repost it, share it on social media, or share links leading to such information.

5. Safety of Products and Services

This incident involved a cyberattack targeting the Company's internal systems and did not target its products and services, including smart meters.
The Company has confirmed that this incident did not affect its production equipment, and no impact on the operation of products and services in use by customers has been identified.

6. Impact on Group Companies

(1) Facts identified: The Company has confirmed that Osaki Electric Systems Co., Ltd. was subjected to unauthorized access via the same VPN device used for the intrusion into the Company, on the same day the Company was attacked (November 15).

(2) Status of investigation: The impact on group companies on the same network is currently under investigation in cooperation with external specialists.

(3) Other group companies: No damage has been identified to date at group companies that are not on the same network (such as Enegate Co., Ltd. and EDMI Limited). Should the situation change, the Company will promptly announce it through its official website and other means.

7. Impact on Financial Results

The impact on the Company's financial results (including any estimated amount) is undetermined at this time, as it will depend on the status of the resumption of operations and the findings of the investigation. Should any matters requiring disclosure arise, the Company will announce them through timely disclosure and other means.

8. Future Actions

Should any new facts requiring disclosure come to light, including the status of the resumption of operations or the findings of the investigation into the information leakage, the Company will promptly announce them through its official website and other means.

9. Requests to Customers and Other Parties Concerned

(1) If you have any questions or concerns regarding delivery schedules for existing orders or future orders, please contact the relevant business division or Purchasing Department of the Company.

(2) If you receive any suspicious emails purporting to be from the Company, please do not open any attachments or click on any URLs contained in such emails. If you receive any suspicious telephone calls, please end the call without providing personal information or other details. In either case, please notify the contact listed below.

The Company once again sincerely apologizes for the significant inconvenience and concern caused to its customers and all other parties concerned.

[Contact for inquiries regarding this matter]

Customers and business partners:

Please contact the relevant business division or Purchasing Department of the Company.

Media inquiries:

Corporate Communications Department, pr_all@osaki.co.jp