Nidec Corporation

June 10, 2024

Security Incident at a Nidec Group Company

Nidec Corporation ("we" or the "Company") today announced that Nidec Instruments Corporation ("Nidec Instruments"), a Nidec Group company, has suffered a ransomware attack. We deeply apologize for all the inconveniences and concerns that this incident has caused to our business partners and others concerned.

Though no damage to the Company or any other members of the Nidec Group has been confirmed, we will implement measures for early recovery from this incident, enhance the entire Nidec Group's information security system, and launch actions to prevent future similar cases.

Please see the next page for Nidec Instruments' announcement regarding this incident.

Nidec Instruments Corporation

June 10, 2024

Security Incident at Nidec Instruments Corporation

This is to inform that Nidec Instruments Corporation ("we" or the "Company") has been subjected to a cyberattack by an external malicious group on May 26, 2024, which resulted in multiple files in the Company's server being encrypted. In the wake of this ransomware incident, the Company has established a company-wide task force to receive advice from outside experts, while investigating the impact of this matter and proceeding with recovery efforts. In addition, the Company initiated consultation with the police and other organizations concerned immediately after the incident occurred, to receive advice on countermeasures.

Though, at present, the specific extent of the data breach has yet to be identified, we will investigate this matter thoroughly, and launch any and all measures necessary for an early clarification of the attack and prevention of future similar incidents.

Lastly but not the least, we deeply apologize to our business partners and related parties for the tremendous concerns and inconveniences caused by this criminal act, which has caused severely impaired our internal business operations. Going forward, the Company will invest all of its resources required to solve this matter promptly and appropriately, and do its very best to do so by regarding information security as our top priority.

-###-