

**October 11, 2024**

MURAYAMA INC.

President and CEO: Yukimasa Saiki

### **Report on Additional Measures Regarding the Security Incident**

Regarding the security incident that occurred on July 14, 2024, Murayama announces that it has concluded a thorough investigation and determined that the likelihood of a data breach is extremely low. In compliance with relevant regulations, we are issuing this notification to our business partners and related parties.

We have notified the supervisory authorities in Japan and the EU within the timeframes stipulated by the respective regulations.

### **Overview of the Incident**

On July 14, our company's servers were affected by unauthorized access, which led to the encryption of stored data. Evidence suggests that the attack was carried out by exploiting our VPN functions to access our network, and it was confirmed that multiple devices within the network were also attacked. Consequently, we investigated the affected servers for signs of data leakage and examined records of data communication through various routes to and from external sources.

### **Data Breach**

No evidence of data leakage has been found on the affected servers, and no facts confirm any actual leakage. Additionally, communication logs indicate that the volume of data transmission during the breach was minimal. As of now, there is no indication that any data has been improperly made public. Based on these findings, we have concluded that the likelihood of a data breach is extremely low.

However, since we cannot completely rule out the potential for data leakage or access by attackers, we are issuing this notification in compliance with relevant laws in Japan and the EU.

### **Personal Data Involved**

Although the data stored on the affected servers was encrypted by the attackers, we have determined that the following personal data may have been included:

- Data of business partners and related parties (names, organization names, department names, business contact information.)
- Data of current and former employees (names, addresses, birthdates, insurance numbers, etc.)
- Data in construction logs and worker rosters of contracted projects (names, addresses, birthdates, insurance numbers, blood types, etc.)

We will notify the affected individuals via email or letter. For any questions, please feel free to contact us at the email address provided at the end of this release.

### **Security Measures Implemented**

In response to the security incident, we have implemented the following actions to safeguard our systems and data:

- Disconnected compromised servers and PCs from the network
- Initialized compromised devices
- Strengthened password policies
- Discontinued compromised VPN routes
- Reconstructed the Active Directory (AD) server
- Reorganized the internal structure for information management

We will continue to maintain our response task force and take swift action should any new developments arise, and we will report to all concerned parties accordingly.

We sincerely apologize to our business partners and related parties for the significant inconvenience and concern caused by this security incident. We take this matter seriously and are committed to building a secure environment for our business partners.

### **Contact Information**

MURAYAMA INC. Security Incident Response Headquarters  
murayama-pr@murayama.co.jp