### Text  Description automatically generated with medium confidence

### Data breach response plan

*The purpose of this document is to outline guidelines and procedures needed in the event of a cybersecurity incident. Store this document in several locations. It should remain accessible to all members of the computer security incident response team (CSIRT), even if all communication systems and the main corporate network go offline.*

**This document does not include information on how to identify or contain a breach. It should only be used once an incident has officially been deemed a breach.**

### CSIRT members

*All areas of the business must be represented. In the event of a confirmed incident, this team should convene as soon as possible to determine follow-up actions. Suggested job titles that should be involved include:*

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Telephone | Email address |
|  | CEO |  |  |
|  | CFO |  |  |
|  | CIO |  |  |
|  | CISO |  |  |
|  | Head of legal |  |  |
|  | Head of marketing |  |  |
|  | Head of people |  |  |
|  | Head of IT |  |  |
|  | Infrastructure manager |  |  |
|  | Head of client relations |  |  |

### Contact list

*List third-party companies and authorities who should be contacted in the event of an incident.*

|  |  |  |  |
| --- | --- | --- | --- |
| Company name | Company role | Contact name | Contact phone |
|  | Cyber insurance |  |  |
|  | Incident response (cybersecurity consultancy) |  |  |
|  | Regulatory authorities |  |  |
|  | Law enforcement |  |  |

### Incident steps

*This section shows the steps to take during a cybersecurity incident. This should be customized based on your industry sector and geographical location, as there may be different regulatory authorities you need to contact. Add specific details as needed for your business.*

|  |  |
| --- | --- |
| Action | Action owner |
| Initial responder raises incident to incident response group. |  |
| Is the incident real?  |  |
| If incident is real:* Activate incident response group
* Contact cyber insurers and cybersecurity consultancy for expert help and advice
* Keep a detailed log of all actions from this point
 |  |
| Has the incident been contained? If not, initiate containment and eradication procedures. |  |
| Has data been encrypted or deleted? If so, activate data recovery procedures. |  |
| Has confidential data been stolen? If so, inform affected parties using prepared statements. |  |
| Inform regulatory authorities if needed. |  |
| In the event of a ransomware attack:* Is data recoverable in an acceptable time frame?
* Consider at this point whether to negotiate with cybercriminals. Any negotiation must be done in agreement with your cyber insurance provider.
 |  |
| Will the media know about the incident? If so, release the prepared media statement. |  |
| Discover how the breach occurred and mitigate any issues.* Use third-party data forensics to help with this process.
* Change passwords of all accounts in all systems.
 |  |
| Decide whether you wish to involve law enforcement. |  |
| Ensure client account managers speak to affected clients to reassure them and provide information as required. |  |
| Evaluate the response to the incident and improve plan where necessary. |  |

### Communication plans

**Regulatory authority statement:**

**Client statement:**

**Staff statement:**

*Include below prepared statements for staff, clients, media and regulatory authorities. You may want to prepare multiple statements for each type of incident.*

**Media statement:**