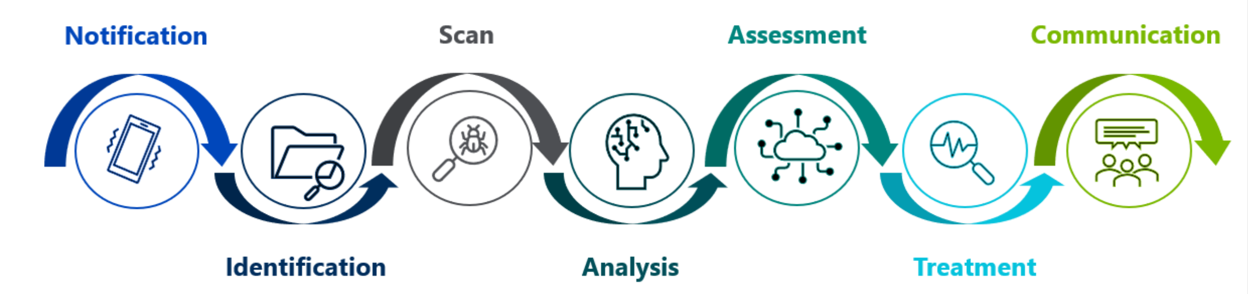
Nuremberg, January 29, 2021 **| PUBLIC**

Landis+Gyr Vulnerability Management Policy Summary

As a provider of products and services, Landis+Gyr focus on protection of the customer's privacy and security. This policy was created for customer guidance and information in the event of a potential or detected vulnerability in a Landis+Gyr product or service. This document provides the information how Landis+Gyr responds to events of this nature.

1 | Vulnerability Handling

Landis+Gyr has a separate cyber emergency response team (CERT) which focuses on Landis+Gyr enterprise, products services: the Landis+Gyr productCERT team. This team ensures a proper handling of each reported topic, which includes the following steps:



2 | Notification

Landis+Gyr encourages all external parties to notify Landis+Gyr about potential or suspected vulnerabilities.

In case a customer, a service provider, or any external person suspects or discovers a vulnerability, the information should be reported via the following Landis+Gyr security web page:
https://productcert.landisgyr.com/

With the help of this web page, several pieces of information can be provided in a structured way. It is also possible to attach files which can help Landis+Gyr to better understand the scenario and the potential consequences of a vulnerability.

Landis+Gyr likes to get in contact with the finder of a vulnerability in order to better identify the vulnerability. However, Landis+Gyr supports a finder who wants to stay anonymous: a corresponding check box on the web page mentioned above can be flagged accordingly.

Landis+Gyr encourage reports to encrypt sensitive information via usage of the public Landis+Gyr PGP key, in order to securely disclose sensitive or confidential information about products and services. The PGP key as well as fingerprint is published on the mentioned web page above.

For general security topics, please contact the Global Cyber and Information Security team by sending an email to: cybersecurity@landisgyr.com

3 | Identification of Vulnerabilities

Landis+Gyr uses several mechanisms to identify suspected or discovered vulnerabilities, e.g.

- Internal reporting mechanisms (perform security audits, perform process reviews, encourage internal employees and contractors to raise security tickets, etc.).
- External security reporting mechanisms (provide public web interface to allow vulnerability notifications, oversee supplier notifications, monitor security news boards, handle interested party security alerts, etc.).
- External penetration testing.

4 | Scan for Vulnerabilities

In addition to the above-mentioned mechanisms, Landis+Gyr uses several automated methods to detect vulnerabilities, e.g.

- Regular vulnerability scanning of network, code, and endpoints.
- Systems are scanned for well-known and newly discovered vulnerabilities.
- Software is checked for vulnerabilities by automated triggered test cases.

5 | Analysis

Each suspected or discovered vulnerability is submitted to the global vulnerability tracking tool. Each suspected or discovered vulnerabilities will be analyzed and grouped, e.g.

- Newly discovered or zero-day vulnerability.
- Already known vulnerability.
- Security question.
- Spam.

Each vulnerability is further evaluated and checked for:

- Affected software type and version.
- Affected device type and firmware version.

6 | Assessment

The productCERT team as well as additional experts will assess and evaluate all vulnerabilities. The experts are from various departments, e.g. Cyber and Information Security, Data Privacy, Product Management, Product Management Security, R&D, etc.

Landis+Gyr uses two methods for this purpose:

- The Common Vulnerability Scoring System (CVSS), version 3.1.
  The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. It includes three metric groups “Base Metric Group”, “Temporal Metric Group” and “Environmental Metric Group”.
- The Common Criteria for Information Technology Security Evaluation (CC), version 3.1 release 5. The CC is an international standard for computer security certification: ISO/IEC 15408. This methodology includes evaluation of a vulnerability for “Elapsed Time”, “Expertise”, “Knowledge of the Target of Evaluation”, “Window of Opportunity” and “Equipment”.

Landis+Gyr uses the following criticality classification scheme:

- **CRITICAL** | 9.0 – 10.0 in CVSS v3.1
  Vulnerabilities can be compromised with publicly available malware or exploits.
  Compromise would have severe or major consequences to Landis+Gyr or its customers or partners.
- **HIGH** | 7.0 – 8.9 in CVSS v3.1
  There is no known public malware or exploit available.
  Compromise would have severe consequences to Landis+Gyr or its customers or partners if exploited.
- **MEDIUM** | 4.0 – 6.9 in CVSS v3.1
  There is no known public malware or exploit available.
  Compromise would have moderate consequences to Landis+Gyr or its customers or partners if exploited.
- **LOW** | 0.1 – 3.9 in CVSS v3.1
  Compromise would have minor or no consequences to Landis+Gyr or its customers or partners if exploited.
- **INFORMATION** | 0.0 in CVSS v3.1

7 | Treatment

The treatment of an identified vulnerability will be done in an appropriate way to minimize or eliminate the risks of exploitation. Landis+Gyr is committed to improving its products and services. Due to various complexity of remediations/mitigations, the schedule for provisioning of these will be determined for each vulnerability separately.

The treatment consists of following phases:

- Prioritization of the Vulnerability
  As several vulnerabilities and security flaws exist, it is important to focus on the most critical ones, based on its impact to Landis+Gyr and its customers.

- Decision on Treatment
  Landis+Gyr uses four categories:

Remediation:	Threat can be eradicated or completely removed.
Mitigation:	Changes to minimize the impact or ability to exploit.
Avoid:	Actions taken to now allow the vulnerability to be exploited.
Accept:	Vulnerabilities with minimum impact can exist as is.

- Perform Treatment
  The defined treatment will be performed and validated. Examples for remediation are to provide a patch, to suggest a new firewall rule or to adapt an existing one, to change protocols or protocol versions, etc.

8 | Communication

Landis+Gyr believes that both Landis+Gyr as well as the finder of a vulnerability must act responsibly and with ethical intentions to improve the industry. This includes that, by default, a vulnerability will be kept confidential and must not be made public without consent.

Landis+Gyr will perform the following external communication:

- Acknowledgement of submitted reports in a timely manner.
- Communication with the reporter during analysis of vulnerability.
- Communication to all affected customers in a timely manner via sending Security Advisory email(s), which will include CVSS or CC scoring, description, affected products and systems, etc.
- Based on consent, the reporter will be acknowledged in the Security Advisory emails.

Landis+Gyr will perform internal communication according to the defined vulnerability management process to ensure a fast and proper handling of vulnerabilities.

9 | Terms and Abbreviations

Terms used:

- Threat — A possible attack to a product or system.
- Vulnerability — A weakness of a product or system which could be exploited by a threat.

Abbreviation list:

CC:	Common Criteria for Information Technology Security Evaluation (https://www.commoncriteriaportal.org/cc/)
CVSS:	Common Vulnerability Scoring System (https://www.first.org/cvss/)
IEC:	International Electrotechnical Commission
ISO:	International Organization for Standardization
productCERT:	Product Cyber Emergency Response Team
PGP:	Pretty Good Privacy
R&D:	Research and Development