Landis+Gyr AG
Theilerstrasse 1
Postfach 260
6301 Zug
Switzerland

Landis+Gyr
manage energy better

Zug, September 6, 2016 | **PUBLIC**

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

G-IS-POL005-Vulnerability_Disclosure

Department	Information Security
Version	1.0
Classification	PUBLIC
Printed Date	2016-09-09
Author	Thomas Mosel
Approved by	productCERT, Group Security Committee
Approval Date	2016-09-20
Status	APPROVED
Reference-ID	G-IS-POL005
Name	Vulnerability Disclosure

The electronic file is the official version and supersedes any printed version.

Landis+Gyr
manage energy better

Table of Contents

1 | Version Control

Version	Date	Author	Details
1.0	2016-09-06	Thomas Mosel	Initial Revision to publish on website.

2 | Related Standards

Standard
ISO/IEC 29147:2014 Vulnerability Disclosure
ISO/IEC 30111:2013 Vulnerability Handling

3 | Terms and Abbreviations

Term/ Abbreviation	Definition
productCERT	Product Cyber Emergency Response Team
PGP	Pretty Good Privacy
Threat	Possible attacks to products, systems
Vulnerability	Weakness of a product or systems which could be exploited by a threat.

4 | Purpose

Landis+Gyr is committed to resolving vulnerabilities to meet the needs of its customers and the broader technology community. This document describes Landis+Gyr's policy for receiving reports related to potential security vulnerabilities in its products and services and the company's standard practice with regards to informing customers of verified vulnerabilities.

5 | When to contact the Product Cyber Emergency Response Team

Contact the Landis+Gyr **Product Cyber Emergency Response Team** (productCERT) by sending email to productCERT@landisgyr.com or report via https://productCERT.landisgyr.com in the following situations:

- You have identified a potential security vulnerability with one of our products
- You have identified a potential security vulnerability with one of our services

After your incident report is received, the appropriate personnel will contact you to follow-up.
To ensure confidentiality, we encourage you to encrypt any sensitive information you send to us via e-mail. We are equipped to receive messages encrypted using PGP. A copy of the certificate (**5FEE B70F F9BE 677D 161C 2031 430B 9F8A D15A 9F9C**) that can be used to send encrypted email can be found on our website with this policy under https://productCERT.landisgyr.com.

The productCERT@landisgyr.com email address and the https://productCERT.landisgyr.com website are intended ONLY for the purposes of reporting product or service security vulnerabilities. It is not for technical support information on our products or services. All content other than that specific to security vulnerabilities in our products or services will be dropped. For technical and customer support inquiries, please visit our company website or contact directly your customer support.

Landis+Gyr attempts to acknowledge the reception of submitted reports within two working days.

6 | Receiving security information from Landis+Gyr

Technical security information about our products and services is distributed through several channels depending on the customer contract and the product or service.

In most cases, we will issue a notice when we have identified a practical workaround or fix for the particular security vulnerability though there can be instances when we issue a notice in the absence of a workaround when the vulnerability has become widely known to the security community. As each security vulnerability case is different, we can take alternative actions in connection with issuing security notices. Landis+Gyr does not guarantee that security notices will be issued for any or all security issues customers can consider significant or that notices will be issued on any specific timetable. Landis+Gyr can determine to accelerate or delay the release of a notice or not issue a notice at all. Generally, we do not disclose vulnerabilities publicly.

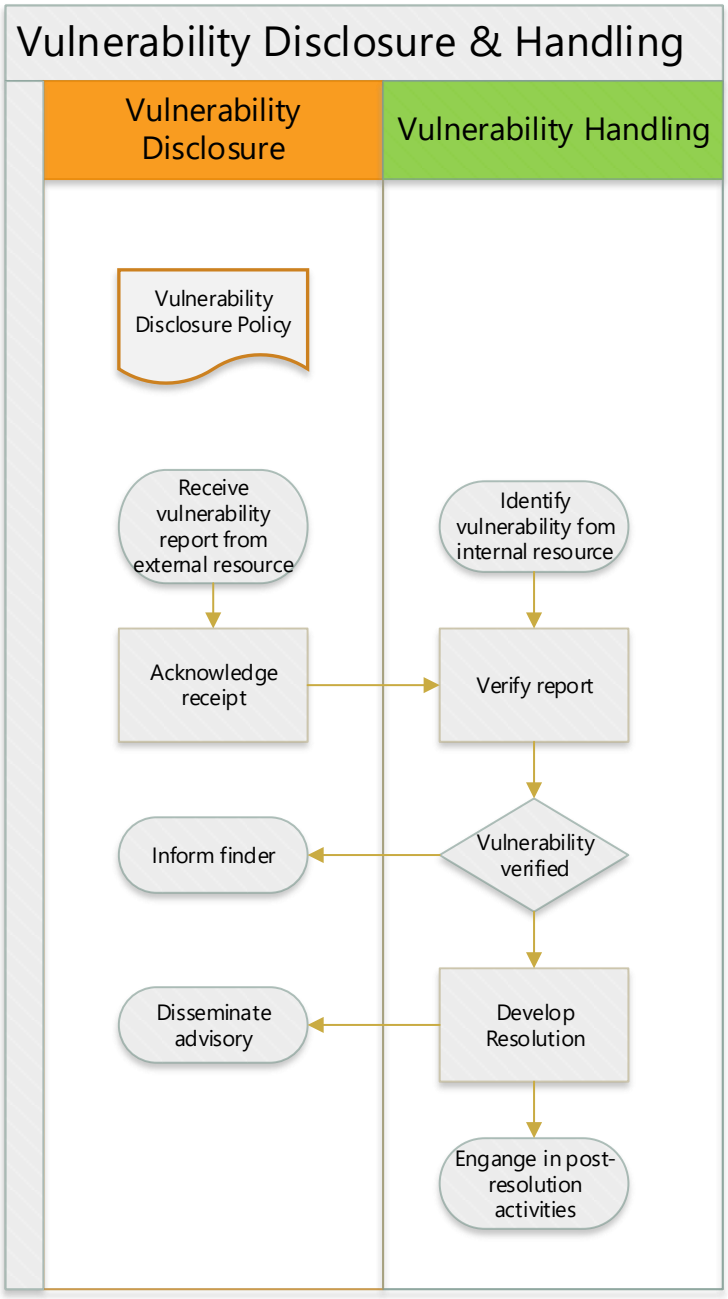

Figure 1: Process Overview