FY18 Global Information Security Policy

AVNET
Reach Further™

A vision to keep Avnet's information and systems safe.

Towards a safer Avnet

TEAM AVNET,

Welcome to the FY18 edition of the Avnet Global Information Security Policy, or GISP.

The world of information security changes quickly, as security experts, vendors and organizations work together to stay one step ahead of malicious hackers and information thieves around the globe. The GISP is a foundational element of Avnet's information security strategy, containing the latest best practices, policies and procedures designed to keep confidential company, employee and customer information secure in all of our business activities.

While much has changed over the last 12 months in information technology, one thing has remained constant: you, the Avnet employee, will continue to be the primary target for data thieves and hackers. So it's essential that every one of us is committed and equipped to serve as a responsible user of Avnet's information technology, security and communication resources.

This document gives you the understanding needed to fulfill that responsibility effectively. The guidelines and policies outlined in this GISP are designed to both protect and empower you, enabling you to do your part to ensure that Avnet's people, systems and data remain secure at all times.

I would encourage you to contact the GIS Security team at GIS.Security@Avnet.com with any questions or concerns related to the safety of our people, systems and data—including any suspicious emails, calls or activity you may encounter in your business activities.

Thank you for your commitment to reading, understanding and upholding the GISP in the months ahead—working together, we make a safer Avnet.

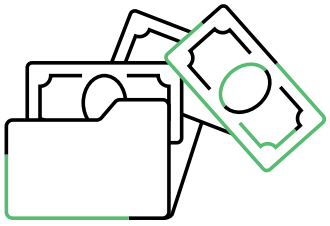
MJ RAO
VP Enterprise Architecture and Information Security
Avnet, Inc.

Table of contents

GISP overview

The purpose of this Global Information Security Policy (GISP) is to provide guidelines and procedures to protect the information technology, security and communication resources—such as information data, hardware, systems and software—of all of the business units of Avnet, Inc. and its subsidiaries ("GIS Resources").

Through the selection and application of appropriate safeguards, this GISP supports Avnet's mission by outlining strategic practices that protect our physical and financial resources, reputation, users and other tangible and intangible assets.



$121 MILLION:

estimated haul for one gang of ransomware hackers in the first half of 2016 alone.

"2017 Security Predictions" Forcepoint Security Labs

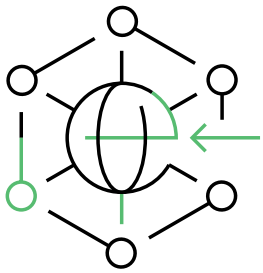
OBJECTIVES

- Maintain the confidentiality, integrity and availability of Avnet's information by safeguarding the information contained within GIS Resources.
- Protect information belonging to Avnet, our employees and our partners.
- Protect GIS Resources and investments against accidental, inappropriate or unauthorized use, modification, loss or destruction.
- Minimize and manage risk to Avnet and Avnet stakeholders.
- Protect the good name and integrity of Avnet and the Avnet brand.

SCOPE

This GISP applies to all users of Avnet's GIS Resources.

- This GISP is socialized during new user orientation, and requires formal acknowledgement in order to gain and retain access to GIS Resources.
- This GISP is updated and acknowledged annually.
- This GISP is the Avnet global default policy. Although regional GIS Security policies are not authorized, regional amendments to this GISP may be coordinated and documented by GIS Security through an approved exemption request, an Appendix to the GISP, or in the GIS Security Standards.
- Avnet reserves the right-consistent with local law-to monitor and review the use of GIS Resources, and to take action concerning potential, actual or suspected violations of Avnet's applicable policies or unlawful acts. Given these situations, in order to maintain security, monitoring may capture business and personal information.
- Exceptions to this GISP require an approved exemption request form. Exemption requests are documented through this GISP exemption approval process.
- Any user found to have violated this GISP may be subject to disciplinary action, up to and including termination.
- The GISP is not intended to create a contract of employment between Avnet and any of its users.
- This GISP does not supersede or replace laws and regulations.
- Avnet reserves the right to modify this GISP at any time.



GAPS IN IoT DEVICES

exposed the largest DDoS attack in history via Mirai botnet

"2017 SonicWall Annual Threat Report" SonicWall

Definitions

This GISP incorporates the standards, guidelines and other documents that can be found in the GIS Security Standards.

POLICY:

This Global Information Security Policy together with the GIS Security Standards are determined by GIS Security and applies to all users globally.

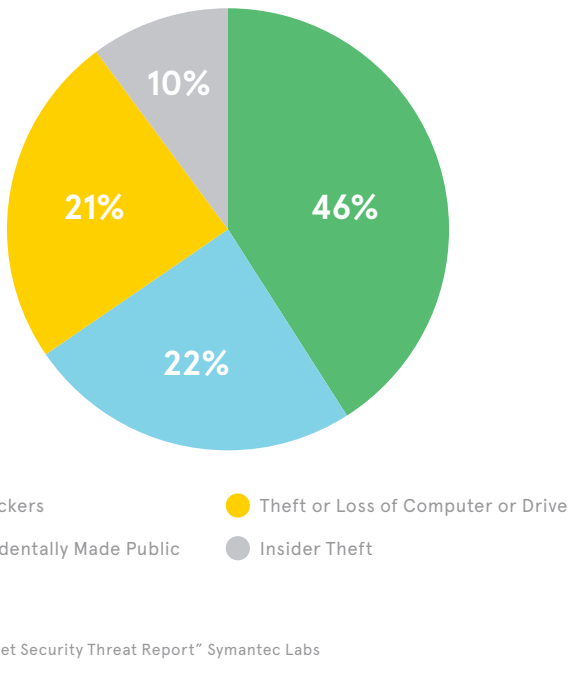
STANDARDS:

These standards are supplements to this GISP and will apply as determined by GIS Security.

GUIDES AND PROCEDURES:

These guides, procedures and supporting documents are the operational step-by-step methods to implementing various standards to comply with this policy. Guides are specific to the particular hardware, software applications, operating systems, tools and architecture.

Top causes of data breaches by incident



"2016 Internet Security Threat Report" Symantec Labs

Responsible use: A call to action

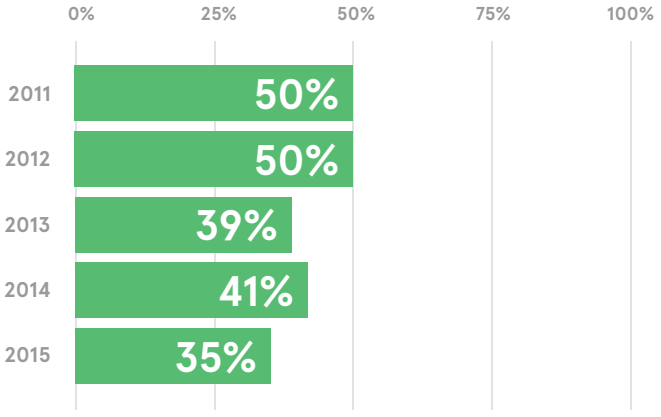
The set of guidelines below is designed to help all Avnet users be more productive, protected and proactive in the business interactions we conduct online, regardless of the tools and technologies we use.

- Review and follow the Global Information Security Policy (GISP).
- Think before your click. There is no such thing as "free". If something seems too good to be true, then it probably is.
- Do not open email attachments, or click on links or popup messages from people you don't know.
- Manage your information as if it is "confidential".
- Help protect communications with regard to identity, privacy and intellectual property.
- Do not share personal information with anyone you do not know.
- Help mitigate risks by being perceptive and insightful in your interactions and communications.
- Store your files in Avnet-approved storage or cloud collaboration locations that meet GIS Security and encryption standards. Do not store Avnet information in personal or public cloud solutions.
- Do not write down passwords or keep passwords where they can be found.
- Create difficult-to-guess but easy-to-remember passwords.
- Do not use passwords that are:
  - Words in a dictionary.
  - A derivative of user access IDs.
  - Common character sequences such as "A1B2C3".
  - Tied to personal information such as spouse's name, license plate, social security number and birthday.
  - Proper names, geographical locations or common acronyms.
- Do not give or share your password with anyone.
  - The only case where this is allowed is when working with Avnet GIS Service Desk on an existing problem ticket. Immediately change your password when the issue is resolved and the ticket is closed.
- Lock your desktop workstation when not in use.
- Use privacy screen protectors and position display screens in such a way thatthe view is obscured from unauthorized persons. Report any suspicious or nonstandard activity to your supervisor.

"Tech support" scam incidents

"2016 internet Security Threat Report" Symantec Labs

Percentage of spearphishing attacks on large companies (2,500+ employees)



"2016 Internet Security Threat Report" Symantec Labs

Acceptable use

All users share GIS Security responsibilities to assist in maintaining the GIS Resources in accordance with Avnet-approved processes. The user's responsibilities include:

- Users are responsible to follow applicable GIS Security Standards and comply with all applicable laws and regulations.
- Users will not attempt to compromise or circumvent Avnet security measures.
- Users will use GIS Security approved resources and tools, technologies and solutions.
- Users will use GIS Resources primarily for Avnet's business purposes and workrelated issues.
- Users will not use GIS Resources for the creation, solicitation, promotion or distribution of any non-Avnet business or for activities that may be illegal, offensive, disruptive, harmful or otherwise prohibited by applicable company policies.
- Users are allowed limited and reasonable personal, non-business use of GIS Resources, provided that such use is not an abuse of company time or these resources, and does not limit Avnet's ability to review data on GIS Resources.
- Users are encouraged to use non-Avnet email service providers for personal/private email, and to remove personal correspondence and documents from the company's GIS Resources.
- User access ID and passwords will only be used by the assigned user and every user is responsible for all activities conducted under his/her user access ID.
- Users are responsible to save Avnet-related documents and data to a network location that is backed up and maintained by GIS.
- Users are responsible to store all Avnet information in Avnet-approved storage solutions, including cloud collaboration locations and encrypted portable storage devices that meet GIS Security and encryption standards.
- Do not use personal or public cloud solutions, or portable storage devices that have not been approved by GIS Security, including USB storage drives (flash drives), memory cards, mobile phones, DVDs, personal backups or home backups.
- Users will acquire and use software only through Avnet processes and authorized licensing.
- Users will not disable, remove or alter Avnet installed software.
- Users will comply with all processes designated to help protect and prevent unauthorized access, use or theft of Avnet resources, devices or systems.
- Users will protect confidential and personal information.
- Confidential information may only be disclosed to persons who are specifically authorized by Avnet to receive the information.
- Users will report GISP threats, incidents or violations to their manager and their GISP regional representative listed in this document.
- Users will report all suspected system intrusions, malware, malfunctions and any other conditions that might jeopardize GIS Resources to their manager and their GISP regional representative listed in this document.

"With their multiple social media accounts, millennials present hackers an expanded attack surface."

"2017 Security Predictions" Forcepoint Security Labs

If you have an Android device use these settings to avoid malware:

Install applications from unknown sources

Verify applications

"2017 SonicWall Annual Threat Report" SonicWall

AVNET-ISSUED DEVICES

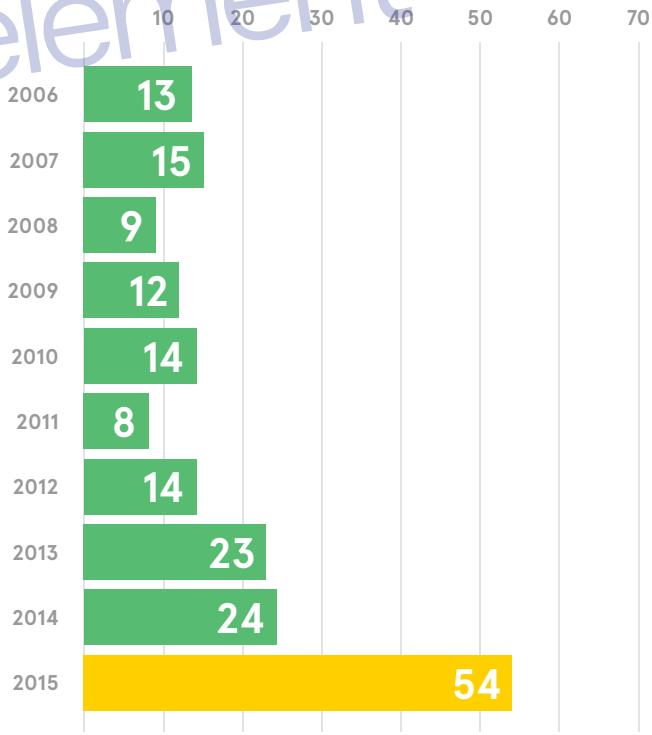
- Users will take reasonable precautions and efforts to secure Avnet-issued devices from theft or damage. International travel may require extra precautions, regardless of your country of origin.
- If the device cannot be kept in a locked facility, then apply additional safeguards, such as taking the Avnet device home each night, securing the device with a cable lock, or locking the device in a cabinet or cupboard.
- Devices will not be stored in vehicles for extended periods of time.
- Devices will be transported in an appropriate case to avoid loss and/or damage.

NON-AVNET-ISSUED DEVICES: BRING YOUR OWN DEVICE (BYOD)

- BYOD devices can include, but not be limited to: laptops, phones and tablet computers that are owned by the user and used to access GIS Resources.
- BYOD devices will either be taken home or will be kept in a secured area.
- When BYOD devices access GIS Resources the Avnet-approved access program will be used.

"Zero day" vulnerabilities by year

A "zero day" vulnerability is a security hole in software that is discovered and exploited by hackers before the vendor can fix it.



"2016 Internet Security Threat Report" Symantec Labs

User authentication and session restriction

Users will help ensure that passwords are constructed and protected in such a way as to provide reasonable safeguards against easy compromise.

- Users will not share or reveal passwords.
- It is acceptable to provide your password to obtain GIS support. Upon conclusion, the user will change their password prior to use and continued access.
- Avnet passwords are for use only with Avnet-managed systems.
- Default passwords provided with new hardware, software or data migrations will be changed prior to use and continued access.
- Initial passwords established, used and issued by GIS Security administrators will be changed prior to use and continued access.

PASSWORD GUIDELINES

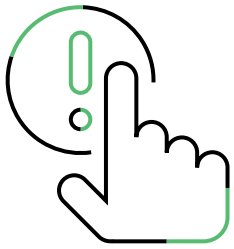
- Minimum password length is 8 characters.
- Password strength is a combination of length, alphanumeric and/or special characters.
- Password expiration requires that users change their user access ID passwords in GIS authentication systems at least once every 90 days.
- Applications that use password synchronization are allowed an additional 3 days for the synchronization process to complete.
- Password rotation will be required by the authentication systems. Users will not be allowed to reuse the 5 most recent passwords.

ACCOUNT LOCKOUT

- After 5 unsuccessful attempts to enter a password in a 35-minute period, the user access ID will either be:
  - Suspended until reset by a system administrator.
  - Temporarily disabled for no less than 15 minutes.

SESSION TIME OUT

- The screen lock is activated after no more than 20 minutes of inactivity. Unlocking the screen will take place only after the user has provided proper authentication credentials.
- The session time out is no more than 4 hours of inactivity. Re-establishment of the session will take place only after the user has provided proper authentication credentials.



>50%

of data breaches in 2015 were due to internal user error

"2016 Global Threat Report" Forcepoint Security Labs

RANSOMWARE ATTACK ATTEMPTS

2014

3.2 Million

2015

3.8 Million

2016

638 Million

"2017 SonicWall Annual Threat Report" SonicWall

Global security

Global Security regulations are covered by the Global Security Standard Operating Procedures including those relating to identification cards, badges and restricted access areas. For further information on Global Security Standards, refer to the Avnet Global Security Intranet.

- Users will present upon request an Avnet badge or government-issued identification.
- Users authorized to access data centers will be required to cooperate with data center security control procedures.
- Users will report any lost or stolen Avnet-issued or personal device that connects to GIS Resources to Avnet Global Security (Global-Security@avnet.com) and GIS Security (GIS.security@avnet.com).
- Users will take reasonable precautions to secure Avnet devices and their work area, including securing personal property.
- Users will return all Avnet identification, devices, equipment, materials and information at the time of separation or upon request from Avnet.

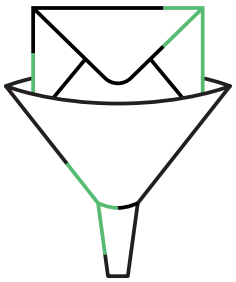
1 IN 5

employees that found unidentified USB drives plugged them into work computers

"2016 Global Threat Report" Forcepoint Security Labs

Security awareness program

There will be periodic security awareness communications to assist in a better understanding of security information, updates, policies, standards, issues, best practices or events.

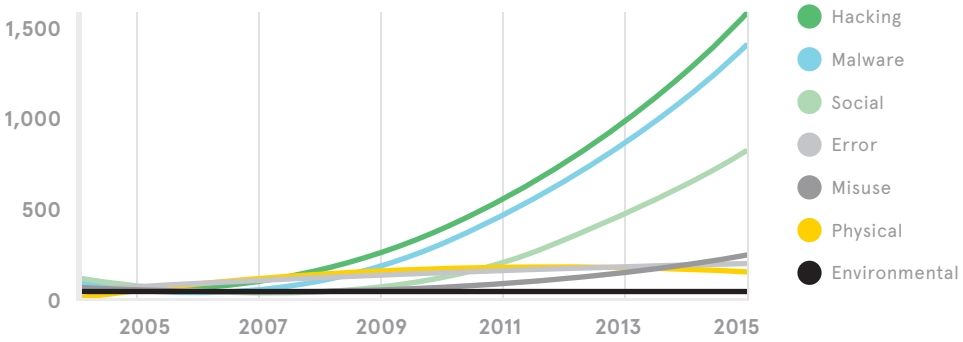


90%

of inbound mail is filtered as spam before it reaches your inbox

Avnet GIS Security, 2017

Data breaches by type



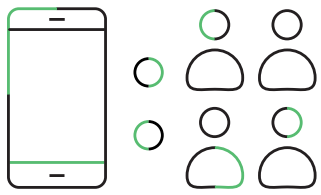
"2016 Data Breach Investigations Report" Verizon

Exemptions to the GISP

GIS Security, GIS management and business unit management will jointly evaluate each exemption request. If the request is not approved, the business unit will continue to comply with the published policy and standards. New and previouslyapproved exemptions will be submitted for review and approval/re-approval annually. An exemption for specific provisions of this GISP does not excuse the requester from compliance with the remaining provisions of this GISP or with other Avnet standards.

Exemptions to the provisions of this GISP may be provided by GIS Security. Business Units requesting an exemption to specific provisions of this GISP will submit an annual request using the online form: GISP Exemption Request Form.

If the exemption is granted, the Business Unit requesting the exemption will be responsible for associated risk, including the documentation of risk management and mitigation controls.



There are now

25 CONNECTED DEVICES

per 100 U.S. residents.

"2016 internet Security Threat Report" Symantec Labs

> "Nearly 50% of organizations reported being targeted by a ransomware attack in the prior 12 months."

"2017 SonicWall Annual Threat Report" SonicWall

Avnet GIS responsibility

Avnet GIS responsibilities to maintain the GIS Resources in accordance with Avnet-approved processes include the following:

- Verifying elevated privileges granted to users based on continued business needs.
- Coordinating business continuity planning with GIS and the business units to provide security and IT disaster recovery capabilities.
- Backing up Avnet data to an Avnet secure data center, or an encrypted storage resource.
- Logging, monitoring and archiving of Avnet system activity may be performed.
- Managing and administering hardware and software.
- Investigating and remediating reported security vulnerabilities.
- Approving and coordinating all activity intended to test GIS Resources.

TOP 5 MALICIOUS EMAIL ATTACHMENT FILE TYPES

#1 .zip
#2 .exe
#3 .txt
#4 .doc
#5 .html

"2016 Global Threat Report" Forcepoint Security Labs

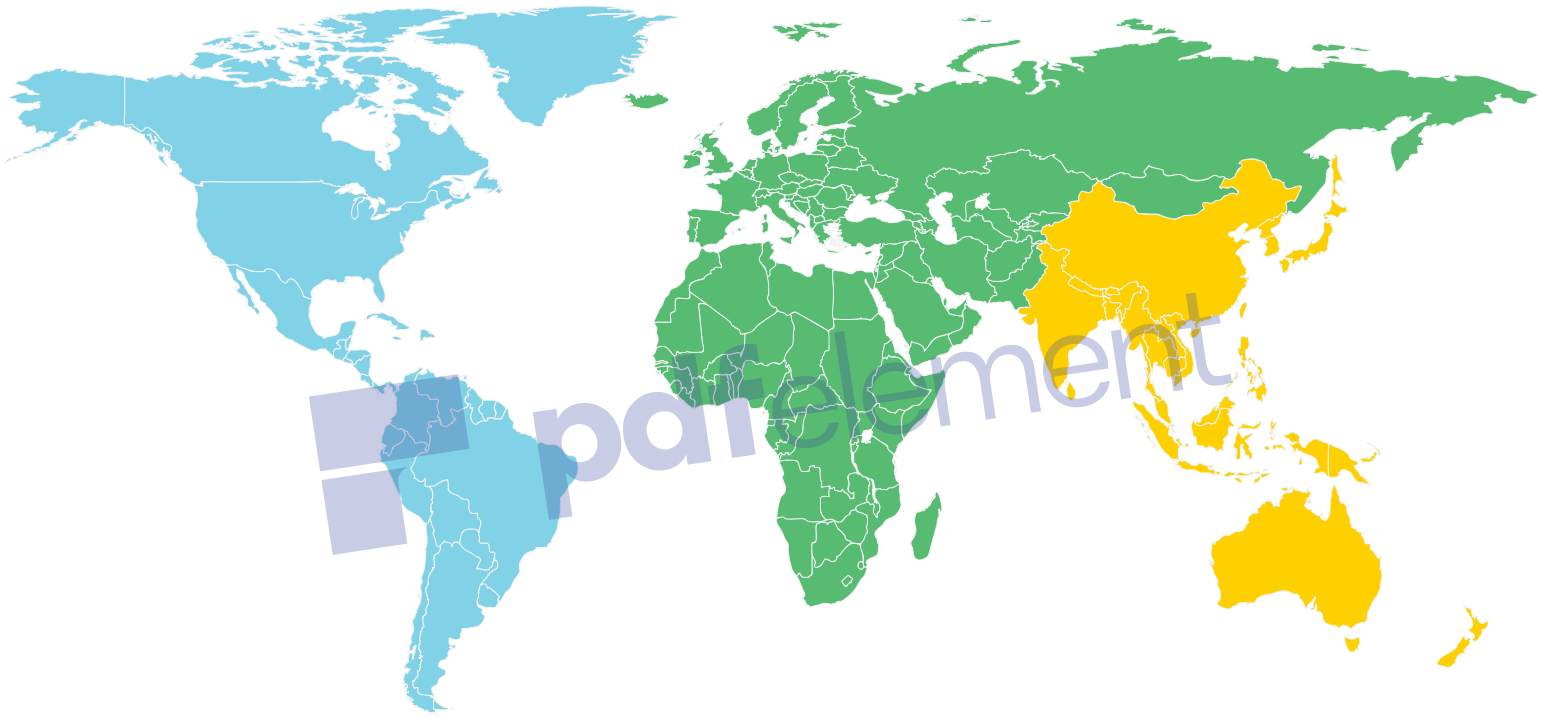
The GIS responsibility are outlined in, but not limited to, the following Security Standards:

GIS Security Standard	GISP Exemption Request	GIS Security Standard	Network Communication
GIS Security Standard	B2B Acceptance of Responsibility	GIS Security Standard	Mobile Communications and BYOD
GIS Security Standard	Risk and Threat Intelligence	GIS Security Standard	Wireless Network Management
GIS Security Standard	Cloud Security	GIS Security Standard	Data and Information Management
GIS Security Standard	Policy Complianc	GIS Security Standard	Business Continuity
GIS Security Standard	Incident Response	GIS Security Standard	Payment Card Industry
GIS Security Standard	Privileged Accounts and Group	GIS Security Standard	Workstation Security
GIS Security Standard	Password Acceptable Use and Management	GIS Security Standard	Data Center Security Access Management
GIS Security Standard	General Data Protection	GIS Security Standard	Web Application Security Integration
GIS Security Standard	Identity Access Management	GIS Security Standard	Leavers Process
GIS Security Standard	Network Access Control (ISE)	GIS Security Standard	Joiners Process
GIS Security Standard	Asset Management	GIS Security Standard	Software Authorization
GIS Security Standard	Application Security	GIS Security Standard	International Travel with a Clean Device

The above links to the GIS Security Standards documents are found in the Avnet Policy Hub - Section 08 - Information Systems and Data Management / Information Security / Standards and Procedures and is subject to change.

GISP regional representatives

Please contact your GISP Regional Representative if you have questions regarding this GISP.



GLOBAL

MJ Rao
Peter Nota
Michael Bish
Dan Porter

AMERICAS

Jayson Flannery
Mark Gildersleeve
Jim Johnston
Trevor Jones

EMEA

Paul Berger
Rudolf Janssen
Alex Obermeier
Peter Nota
Nigel Longbottom

ASIA

Cathy Long
Masao Ebisawa
Sam Ho
Jeff Liu

Acknowledgement of the GISP

ONLINE ACKNOWLEDGMENT:

Users acknowledge receipt of and compliance with the Avnet Global Information Security Policy by completing an online acknowledgment at the intranet acknowledgment portal. Additional regional languages are available on the portal, including: Dutch, French, German, Hebrew, Indonesian, Italian, Japanese, Korean, Mandarin - China (Simplified), Mandarin - Hong Kong (Traditional), Mandarin - Taiwan (Traditional), Portuguese, Spanish and Vietnamese.

PRINTED ACKNOWLEDGMENT:

If the online acknowledgement is not available, use this to acknowledge compliance with the Avnet Global Information Security Policy.

1. Read the Global Information Security Policy.
2. Fill in the form, sign and date in the spaces provided below.
3. Return ONLY the "Acknowledgment of Global Information Security Policy" page to your manager or to GIS Security (GIS.security@avnet.com).

By signing below, I acknowledge the Global Information Security Policy.

Date

User Signature

User Name

User Access ID

Department