Web Governance and Operations Policy

Table of Contents

1 Purpose

The purpose of this document is to define high-level governance and requirements for creation and management of Galderma websites. This policy outlines top level responsibilities and establishes:

1. Galderma's principles and requirements to ensure websites comply with applicable laws, regulations and Galderma's procedural documents.
2. Consistent levels of service, setup, structure, costs, risks, and security.
3. Outline of roles and responsibilities of key stakeholders.

2 Scope

This policy applies to all new and existing Galderma websites. This policy applies to all Galderma employees, agencies, contractors, and other third parties who actively engage in the development, implementation, and maintenance of websites for Galderma. All parties are responsible for reading, acknowledging, and adhering to this and related SOPs and enforcing it throughout the website lifecycle.

All Galderma websites must comply with this policy and all legal and regulatory requirements as determined by Galderma. Website specifications as well as contracts between Galderma and third parties will be reviewed to ensure compliance with this standard prior to execution.

Website content, design, performance, and marketing activities are out of scope for this policy.

This policy will be supplemented by standard operating procedures (SOPs) and working instructions (WIs), as applicable, to provide further information and requirements.

3 References

Documents that should be read in conjunction with or are referenced in this Policy are listed in the following table (document code/title):

[1] SOP: Hosting
[2] SOP: Website Development - Galderma
[3] SOP: Website Development – Agency
[4] POL.00282 Galderma Contract Policy
[5] POL.00256 Global Data Privacy Policy
[6] ITS.10001 Identity and Access Management Standard
[7] ITS.10004 Information Security Incident Management Standard
[8] ITS.10005 Vulnerability and Patch Management Standard
[9] ITS.10007 Records Management Standard
[10] ITS.10008 Application Security Standard
[11] ITS.10009 Third Party IT Risk Management Standard
[12] ITS.10014 Data Management Standard

4 Definitions

4.1 Definitions

Business Owner: holds the budget line on record; responsible for all final approvals

Business Relationship Managers: primary interface between BO and Commercial IT; provides Global IT guidelines and requirements to BO and Agency

Commercial IT: overarching IT business unit that includes BRMs and ITDS; responsible for B2C/B2B CRM, Marketing Automation, eCommerce, payment services, web hosting services, mobile applications, social tools, and back office digital services required for end-to-end service delivery

IT Digital Services: manages operation, configuration, and service delivery for Galderma hosting and DNS; provides guidance and consultation for Galderma websites standards and technical support

Personally-Identifiable Information (PII): including but not limited to first name, last name, email address, phone number, address, IP address, and health information.

4.2 Acronyms

BO: Business Owner
BRM: Business Relationship Manager
CCPA: California Customer Protection Act
CMS: Content Management Systems
DSAR: Data Subject Access Request
DAI: Digital Asset Inventory
GPDR: General Data Protection Regulation
ITDS: IT Digital Services
ITSM: Information Technology Service Management
PII: Personally-Identifiable Information
SNow: Service Now, ITSM
SOP: Standard Operating Procedure
WI: Work Instruction

5 Responsibilities

5.1 Agency

Agency is responsible for all website code development; responding to all requests from hosting service, ITDS, and Galderma IT Security for code changes and optimizations; and Hypercare support activities.

Agency is required to work within hosting platform's environment and requirements; communicate all status changes and needs to BO; create project timeline; develop according to project scope; and get approvals from BO.

5.2 Business Owner

Business Owner (BO) is responsible for project scoping; budget planning and budget validation; agency selection; agency management; deliverables; timelines; approvals; and setting up and following through with any governmental and regulatory reviews.

5.3 BRM

Business Relationship Manager (BRM) is responsible for facilitating communication between all parties; tracking progress on project development; submitting project for security scans; verification of project readiness before website launch; and escalations to any and all parties for any issues.

5.4 Hosting Provider

Hosting Provider is responsible for maintaining a secure server, serving website to customers, providing Helpdesk support with SLA, and monitoring resource usage and service status.

5.5 ITDS

IT Digital Services (ITDS) is responsible for hosting provider selection; providing guidance on CMS; technical consulting; monitoring; and domain and access management.

5.6 IT Security

IT Security is responsible for website security and vulnerability testing, submission timelines, and approval of security plan exceptions. IT Security collaborates with Commercial IT and BO for all remediation plans and are responsible for scheduling and frequency of website scans.

6 Policy

6.1 Project Scope

The project scope defines the purpose of the website, including use case and expected end results from successful launch of website. The project scope includes details about expected end users, type of content, and any necessary website functionality. It must include information on current status of content (already completed vs developed alongside website code) and if a wireframe or design mockup has already been completed. The project scope should not request explicit technical solutions unless referring to required website integrations.

It is BO's responsibility to define the purpose of the website, scope, timeline, and budget. All projects must be communicated to Commercial IT prior to committing resources for engagement with development agency. BO is responsible for communicating all phases of project scope, planning and changes to through Commercial IT BRMs throughout project lifecycle.

All projects must align with Galderma goals, priorities, requirements, and processes. It is the responsibility of all teams working on the project to keep the customer and Galderma's best interests in mind, including ease of use and security as top priorities. BO must work with Commercial IT and other related Galderma departments to develop project scope to ensure all requirements, integrations, and resource needs are included in the project scope and resulting contracts.

All contracts, work, delivered products, and data collection must comply with all legal and regulatory requirements determined by Galderma.

See Website Development - Galderma SOP and Website Development - Agency SOP for further information.

6.2 Inventory

Digital Asset Inventory (DAI) is owned and maintained by ITDS. DAI contains all identifying information and technical details needed to track and maintain all digital assets owned and maintained by Commercial IT. The information is initially populated from the Project Scope and then updated throughout the development process and monthly security scans. DAI has heightened importance for third-party hosted websites as they require extra monitoring and review to ensure compliance and security is maintained.

DAI is used to ensure that all Galderma websites are properly maintained, secure, and included in all systems related to website management such as DNS management services and monitoring. DAI is also used to maintain key stakeholder contact information for incident management and service continuity escalations.

See Website Development - Galderma SOP for further information.

6.2.1 Audit

DAI is audited yearly by ITDS to ensure DAI only contains correct and up-to-date information. The audit will include verification of all information contained within, remediation as needed, and viability review. Website audits may also be executed due to randomized compliance checks, required integrated services updates, legal and regulatory compliance, and at the discretion of Commercial IT and IT Security.

6.3 DNS

Website domains are an important part of Galderma's branding and communication strategy. All Domains must be registered and owned by Galderma. Any domain previously purchased through an external agency or outside of the standard process must be transferred to Galderma's account within Galderma's domain management service within sixty (60) days. Galderma legal must approve any domain that is not an established Galderma brand name. All domain change requests (purchasing, redirects, and deletion) must be submitted via SNow by BRMs.

See Hosting SOP for further information.

6.3.1 URL Format

A properly formatted URL conveys to the customer what information is on the website. Google requires this information to serve the correct country's website; each website follows local law and governance requirements and has country specific products and information.

Galderma has chosen the subfolder method as the primary URL naming convention standard. The subfolder method is www.brandname.com/countrycode-languagecode/.

See Hosting SOP for further information.

6.4 Hosting

A website hosting service provides the storage and services needed to serve a website to the customer. Commercial IT owns all contracts for website hosting platforms. ITDS provides access and provider management.

All websites must be hosted on Galderma approved hosting platforms unless approved by Commercial IT and IT Security. Galderma approved hosting services ensure compliance to basic security and regulatory requirements, secure and consistent servers, and access to helpdesk services.

ITDS will coordinate with BO and BRM to determine which hosting platform best matches the needs of the project. The determination will be based on the purpose of the website as well as any technical requirements. Hosting will include all environments, including development, testing, and production.

Any prebuilt website hosted on third-party hosting platforms must be transferred to a Galderma approved hosting platform to ensure compliance with regional and Galderma determined standards and regulations. Websites outside of Galderma approved hosting environments face increased security and compliance risks. Additionally, they are ineligible for support by Commercial IT outside of basic monitoring.

BO must submit a formal exception request including justification to be reviewed and approved by Commercial IT and IT Security. All exception approvals are time bound and must go through yearly reevaluations. Any exceptions due to budgetary issues must include a plan for transition to Galderma approved hosting and include the required budget in the next budget cycle.

Commercial IT and IT Security have the right to decommission any website due to security risk or noncompliance with regional or Galderma determined laws, policies, and standards. BO will be informed and any website decommissioned due to this determination will be redirected to the domain with the closest content match.

See Hosting SOP and ITS.10009 Third Party IT Risk Management Standard for more information.

6.5 Agency

The website's development agency is a vital part of the success of the project. As such, BO must select a vetted development agency to work on websites. Agency must have prior experience with CMS and be willing to work within Galderma's expectations and requirements. After selection, Agency must agree to read, acknowledge, and follow all website-related Galderma-approved Policies, SOPs, and WIs. Agency must agree to attend training call, follow project scope, and submit to Security Scan. All websites must be developed to operate within limitations of hosting plan.

Agency contract must include Timeline, Scope of Work, defined approval process, Helpdesk, and Hypercare period.

See Website Development - Galderma SOP for further information.

6.6 User Account

Galderma website development must adopt a compliant by design approach throughout all stages and environments, including access management and lifecycle management of user accounts within hosting platforms and websites. User accounts must be assigned to a unique individual and cannot be shared. BO and Agency must inform Commercial IT of any change to user status in a timely manner.

See ITS.10001 Identity and Access Management Standard and Website Development - Galderma SOP for further information.

6.7 Website Development

A successful website relies on clean programming and well-designed content to clearly communicate to customers. Website development is expected to follow Secure by Design principles, OWASP Top Ten standards, and WCAG AA standards. Websites must be kept up to date with the most current security updates.

See Website Development - Galderma SOP, Website Development – Agency SOP, and ITS.10008 Application Security Standard for further information.

6.8 Content Management Systems

Only approved Content Management Systems (CMS) are permitted by Galderma to ensure website security, maintainability, longevity, and brand consistency.

See Website Development - Galderma SOP for further information.

6.9 Data Collection

Customers have the right to know when and why their personal data is being collected. They also have a right to know how it will be used, and to hold Galderma accountable for what happens to their data after it has been collected. There are many laws and regulations established globally to protect personally-identifying information (PII), including GDPR and CCPA. Galderma will be held accountable for any data breaches.

In order to protect both our customers and Galderma, all Galderma websites must follow Galderma's Data Privacy Policy. In summary, all Galderma websites must follow proper data handling and storage procedures. PII must be stored securely and accessed only by authorized users. Only relevant and necessary data should be collected, and data should only be processed for specified, explicit, and legitimate purposes. Electronic records must be securely purged in accordance with Galderma's retention and destruction processes.

Galderma is required to respond to all DSAR inquiries within the designated time period according to local laws and regulations. Any data breaches must follow the process outlined in ITS.10004 Information Security Incident Management Standard.

See POL.00256 Global Data Privacy Policy, ITS.10004 Information Security Incident Management Standard, ITS.10007 Records Management Standard, ITS.10014 Data Management Standard, and Website Development – Agency SOP for further information.

6.10 Security Scan

To keep Galderma properties secure, IT Security will run regular security scans on all live websites to ensure compliance with IT Security standards. Ensuring Galderma's websites are secure and protected is instrumental in protecting Galderma, Galderma's reputation, and the customer experience. These scans are completed on a monthly basis.

Websites are scanned before moving into production. Websites are not allowed to move to production until the security scan is passed

See Website Development – Agency SOP and ITS.10005 Vulnerability and Patch Management Standard for more information.

6.11 Analytics

Website analytics are an important part of data-driven strategy. Galderma websites must be set up with analytics and reporting capabilities using Galderma mandated solutions to collect traffic and other statistics.

See Website Development – Agency SOP for more information.

7 Review

Website Governance documentation must be reviewed and updated:

a) after any changes to Galderma business services
b) after any changes or modifications to Galderma business responsibilities
c) or every 3 years

8 Version History

List the changes made from the last major version, define the measure taken
I = inserted, C = Changed, D = Deleted.

Measure	Section	Describe the change made
C	All	Document creation

Website Development- Agency Standard Operating Procedure

Table of Contents

1 Purpose

The purpose of this document is to define the code level requirements of website development. This standard addresses such functions as code development, environment settings, data collection, security scanning, and analytics. It includes an overview of website development process from beginning to end.

2 Scope

This standard applies to all new and existing Galderma websites. This standard applies to all Galderma employees, agencies, contractors, and other third parties who actively contribute to the development, implementation, and maintenance of websites for Galderma. All parties are responsible for reading, acknowledging, and adhering to this and related standards and enforcing it throughout the website lifecycle.

All Galderma websites must comply with this standard and all legal and regulatory requirements as determined by Galderma. Site specifications as well as contracts between Galderma and third parties will be reviewed to ensure compliance with this standard prior to execution.

Website content, design, performance, and marketing activities are out of scope for this SOP.

3 Definitions

3.1 Definitions

Business Owner: holds the budget line on record; responsible for all final approvals

Business Relationship Managers: primary interface between BO and Commercial IT, provides Global IT guidelines and requirements to BO and Agency

Commercial IT: overarching IT business unit that includes BRMs and ITDS; responsible for B2C/B2B CRM, Marketing Automation, eCommerce, payment services, web hosting services, mobile applications, social tools, and back office digital services required for end-to-end service delivery

IT Digital Services: manages operation, configuration, and service delivery for Galderma hosting and DNS; provides guidance and consultation for Galderma websites standards and technical support

Personally-Identifiable Information (PII): including but not limited to first name, last name, email address, phone number, address, IP address, and health information

3.2 Acronyms

BO: Business Owner
BRM: Business Relationship Manager
CMS: Content Management Systems
DAI: Digital Asset Inventory
DSAR: Data Subject Access Request
EOL: End of Life
ITDS: IT Digital Services

ITSM: Information Technology Service Management
PII: Personally-Identifiable Information
SNow: Service Now, ITSM
UAT: User Acceptance Testing

4 Responsibilities

4.1 Agency

Agency is responsible for providing cost estimate based on project scope; project management and status updates; all development necessary to get environment functioning correctly, including connection to code repository; responding to all requests and incident/outage reports from hosting service, ITDS, and Galderma IT Security for code changes and optimizations including log file management and security changes; and hypercare and support functions after Go Live.

Agency is required to attend all training assigned by Galderma; inform BO when website development is completed; use hosting platform's online documentation for development help; and leverage hosting platform's Helpdesk for any issues.

4.2 Business Owner

Business Owner (BO) is responsible for project scoping, budget planning and budget approval, agency selection, agency management (including most communications), and informing all other parties if there is any need for translations/language support before training. BO is responsible for all agency deliverables and timelines. Content creation is owned and governed by BO. BO is responsible for setting up and following through with any governmental and regulatory reviews. BO is responsible for verifying that all aspects of the project work as requested and communicating all necessary changes to all other parties. BO is responsible for final approvals pre- and post website go live. BO will be expected to complete their final review within ten (10) business days. Any issues after go-live must be reported to the agency during the hypercare period. After Hypercare, BO must raise any issues via SNow ticket or report issues directly to agency for remediation.

4.3 BRM

Business Relationship Manager (BRM) is responsible for facilitating communication between all parties; notifying ITDS of technical changes; communicating status changes to BO; tracking progress on project development; submitting project for a security scan; verification of project readiness before website go-live; and escalations to all parties for any issues.

4.4 ITDS

IT Digital Services (ITDS) is responsible for selecting appropriate hosting provider; providing guidance on CMS; securing domain registration; ensuring project access; setting expectations for project resources; and configuration and management of DNS.

4.5 IT Security

IT Security is responsible for website security and vulnerability testing; submission timelines; approval of security plan exceptions; and are responsible for scheduling and frequency of website scans. IT Security collaborates with Commercial IT and BO for all remediation plans.

5 Requirements

5.1 Code

All websites must be developed to operate within limitations of hosting plan. BO must inform Commercial IT if website resources (such as disk space or RAM) need to be reevaluated.

All code must be developed according to Secure by Design principles and following OWASP Top Ten standards. Code must be optimized for security, speed, and efficiency. All code must be kept up to date with most recent security updates.

5.1.1 Code Lifecycle

All code developed must use current stable release. Code that is end of life (EOL) or within six (6) months of EOL is not permitted for use with Galderma websites.

5.1.2 Content Management Systems

All websites must be developed on one of the following CMS:

1. Drupal (Galderma's CMS of choice)
2. Static HTML

Nonapproved CMS are reviewed individually by Commercial IT according to business request.

5.2 Environment Settings

Agency must use a multi environment workflow with a minimum of three (3) environments. Environments should be named Dev, Test, and Prod.

Agency is required to ensure that all environments are marked as undiscoverable (non-index-able) during development. Each environment must have access limited during development via login credentials or other alternate controls.

All code testing must be restricted to Test or lower environments. Testing or test data is not allowed on Production environment. Testing environment must mirror Production environment for security purposes and to ensure proper testing. Where applicable, any test data must be anonymized and then removed from the database before any code move to Production.

All environments must use HTTPS protocol to ensure compliance with encryption standards.

5.3 File Requirements

Images and other files sizes must be optimized to ensure a balance between image quality and image size, with priority given to a smaller file size. Unused files must be removed within six months after they are no longer in use on website.

5.4 File Management

The database must be optimized to minimize database growth. Log and temp files must have log rotation and/or retention system implemented to limit the amount of space that they take up in the database.

5.5 Data Collection

All websites must follow Galderma's Global Data Privacy Policy and Records Management Standard.

Data collection can occur through the following means:

- Account registration
- eCommerce
- Event Registration
- Savings card signup
- Contact Us form, email, call, or other methods
- Coupons
- Product ratings / reviews
- All other methods not addressed in this list

Any website using these data collection methods must follow proper data handling protocols. BO must include a list in Project Scope of all types of data being collected:

- Type of data collected / Field names
- Purpose of collected data
- Repository for storing data
- Owner of collected data
- Recipients / handlers of collected data
- Access restrictions
- Lifecycle of data
- Method of data transmission to Galderma

All medical data collected must be handled and managed in accordance with local standards and regulations. BO must be able to provide documentation of data collected and implemented compliance methods to regulators upon request or DSAR inquiry.

Galderma Legal is responsible for responding to any DSAR inquiry.

5.6 Language Indicator

Website language must be indicated in URL as well as in HTML header as hreflang tag.

5.7 Website Content Requirements

Links to Legal approved privacy policy and legal policy pages must be accessible on all pages of website. All websites are required to include and display cookies using Galderma approved tools.

5.8 Security Scans

Security Scans are required before a new website is launched or any major code changes are committed to production. Websites are automatically scanned monthly.

Sites not yet in production must remediate all vulnerabilities before site launch. Sites already in production must remediate vulnerabilities within timespan indicated below.

Security scans use four rates to identify site status:

- No or Low vulnerability rate: secure; no development work is needed
- Medium vulnerability rate: not secure; all identified vulnerabilities must be remediated within three (3) months
- High vulnerability rate: not considered secure; all identified vulnerabilities must be remediated within one (1) month

Commercial IT and IT Security must be informed of all changes before code is committed:

- New website launch
- Major code changes
- URL changes

BRM is responsible for submitting ticket to IT Security to kick off any manual security scans. The process has an SLA of five (5) days.

IT Security is responsible for sending results directly to all Galderma and agency members of project. Results are hosted on SharePoint as a html file. Results must be downloaded to view complete results.

IT Security is responsible for answering questions about how to read scan results or how to remediate identified vulnerabilities.

Agencies are required to start working on remediation immediately upon notification. Agency must inform Commercial IT and IT Security if remediation will take longer than established remediation timeline and submit an extension request including justification. IT Security must approve any remediations extension requests.

All sites will be scanned once a month after launch until end of life to ensure continuing compliance. IT Security is responsible for keeping results archive.

5.9 Incidents and Escalation

Agency must respond to site outage or incidents within twenty-four (24) hours. Agency must investigate and then communicate cause and all long- and short-term solutions implemented.

Agency must have assigned Tech Lead to receive and respond to all outage and incident notifications during the entirety of the lifespan of the website.

BRM must be cc-ed in all communications related to incidents.

6 Procedure

6.1 Training

All agencies must agree to attend training. If deemed necessary by BO or Commercial IT, Agency must agree to attend retraining. BRMs are responsible for facilitating training schedules.

6.2 Website Creation

ITDS is responsible for creation of new project on hosting environment and granting access to developers, including all roles and permissions needed to work on project.

Agency will develop all code and implement content as provided by BO. BRMs will keep track of project progress and notify ITDS of any major issues.

6.3 Approvals and Security Scan

Agency is responsible to notify BO once all code development and content implementation is completed.

BO is responsible for verifying all website functions and content behaves as expected. BO must complete testing on recommended devices and browsers. BO must schedule and submit website to all local government and regulatory reviews. BO must inform Commercial IT and Agency of any timeline updates, required remediations, and provide final approval.

BRMs must submit Security Scan to IT Security. IT Security is responsible for sharing scan results to all team members working on website. All Medium and High Security scan results must be remediated before go-live.

Both approvals and security scan must be completed before Go/No-Go call can be scheduled.

6.4 Go Live

BRM is responsible for scheduling Go/No Go call with all team members.

The following requirements must be met before go-live:

- All legal requirements are verified as completed
- Security scan has been passed
- BO verifies website functions as expected
- BO verifies all content is correct and available.
- Analytics container is successfully implemented

BO must provide final approval for website to move to production.

BRM is responsible for coordinating Go-live scheduling with Agency, ITDS, and Hosting Platform as needed.

ITDS is responsible for preparing and validating DNS configuration before go-live.

Agency is responsible for successfully moving code from staging to production.

A least one agency developer (preferably Lead Tech), BRM, and ITDS must attend Go Live call. ITDS must check Hosting Platform’s status to verify hosting platform is not experiencing any service issues prior to call.

Agency, and Hosting Platform as necessary, must make all final updates before ITDS will apply DNS zone change request.

BO and Agency are responsible for confirming proper website functionality after Go-Live.

6.5 Analytics

All websites must be set up with analytics, reporting, and tracking configurations using Galderma owned tools.

ITDS owns access management to all website analytic and reporting tools.

BRM must submit access requests through SNow ticket. Requests for agency access must include first and last name, work email, job title, and agency name.

BO or Agency is responsible for notifying Commercial IT when users no longer need access. ITDS will audit all users on a yearly basis. BO is responsible for validating user list and communicating any changes to ITDS.

BO is responsible for further tagging implementation in alignment with established Galderma strategy and templates.

Basic Project Timeline and Processes for Agency

Project Scope

1. Business Owner works with Commercial IT to develop Project Scope and choose agency.
    a. Work **cannot** be started before the agency contract is signed.
2. Agency must provide:
    a. Data collection access and storage processes and procedures
    b. Hypercare period with detailed communication methods and SLA
    c. Maintenance and security updates for long term websites

Agency Onboarding:

3. All developers are required to attend a hosting platform-specific training to gain access to hosting environment.
    a. Agency must designate a Tech Lead to receive and respond to outage or issue notifications at this time.

Website Development:

4. All website related domains, email addresses, and analytics containers must be owned by Galderma.
5. Developers must use standard GIT tools to manage environments.
    a. Project must use multibranch GIT repo: Dev, Test, Prod.
    b. Non-production environments must be undiscoverable (non-index-able) and limited to login access only.
6. Code must be optimized for security, speed, and efficiency based on current Galderma IT Security and OWASP standards.
7. Project must be developed to operate within limitations of hosting plan.

Code Review:

8. IT Security Scan
    a. SLA of five (5) days; allow at least 3 weeks for remediation.
    b. BRM requests scan when code development is completed.
    c. IT Security communicates all issues and answers any questions.
9. MLR review processes
    a. Business Owner manages MLR process and timeline.

Website Go Live:

10. Code review must be completed before any Go Live processes are scheduled.
11. Final review (Go/No Go) verifies that the website functions, content is correct, and cookies and analytics container is successfully implemented.
12. Go Live includes finalizing code changes to move website to Production.

Website Lifecycle

13. Website will have monthly Security scans.
    a. Agency must start working on remediation immediately upon notification.
14. Any code change must:
    a. include a pre- and post-manual backup.
    b. go through a manual Security Scan **before** any new code is deployed.
15. Any issues that cause website outages or hosting platform notifications must be remediated immediately.
    a. Agency must email an explanation of the issue’s cause and its solution to Commercial IT.
16. Agency must provide archive to Commercial IT at website’s End of Life.