# VORTEX GRID SYSTEMS INC.

## Information Security and Incident Communication Policy

| Document control | Value |
|---|---|
| Record ID | FR-001 |
| Revision | 1.2 |
| Effective date | 2026-04-06 |
| Policy owner | Office of the Chief Operations Officer |
| Approved by | Executive Operations Council |
| Review cycle | Annual, and after a material incident |
| Classification | Internal operating policy |

### 1. Purpose and scope

Vortex Grid Systems Inc. develops and operates software and field services for distributed energy customers. This policy establishes the minimum operating rules for protecting service information, documenting incidents, and communicating with customers and internal teams. It applies to employees, temporary staff, contractors, and approved suppliers who create, receive, store, or transmit Vortex Grid business records. The policy covers office systems, field-service devices, customer-support workspaces, approved collaboration tools, and project documentation.

The objective is not to prevent ordinary engineering disagreement. Teams must be able to record competing technical observations, incomplete information, and provisional recommendations without changing the record after the fact. The objective is to make the scope, author, time, and status of each statement clear enough that later review can distinguish an observation from a conclusion, a correction from an original message, and an approved customer statement from an internal working note.

## 2. Information handling requirements

Business records must be created in an approved system or exported promptly into an approved record format. Each record must identify its authoring organization or team, the creation date, and a stable reference number where one is assigned. A person who forwards or quotes a record must preserve the quoted material as quotation and must not present it as a new observation. If a message summarizes a field report, the message must identify the report reference and the author of the summary. Screenshots or copied tables may assist a review but do not replace the original text or tabular record.

Personnel may use familiar display names in routine communication, but an incident, approval, purchase, or personnel record must include the sender’s directory identity or role. Managers are responsible for resolving ambiguity when two people have a similar display name, a shared surname, or overlapping responsibility. The resolver must not infer identity from a signature alone when the document concerns a material decision. Instead, the record must state the department, role, or employee identifier that establishes which person acted.

## 3. Incident record and escalation process

An incident record begins when a service disruption, safety concern, suspected data exposure, or material customer-impacting defect is reported. The first reporter must create a dated incident entry containing the observed condition, affected service or site, immediate containment action, and any known uncertainty. The entry may use terms such as "reported," "observed," "suspected," or "not yet verified." It must not claim a root cause merely because a likely cause is being investigated.

The duty manager assigns an incident coordinator within one business hour for a severity-one or severity-two incident. The coordinator maintains a chronological decision log, requests technical assessments from relevant teams, and confirms the customer communication owner. Engineering, field operations, and customer operations may each submit findings. Disagreement is recorded as separate attributed findings; the coordinator may not replace one finding with another to create the appearance of consensus. A customer-facing update must identify whether it is an operational status, a confirmed conclusion, or a preliminary assessment.

When an initial conclusion is later found incomplete or incorrect, the responsible executive issues a correction or retraction that cites the prior record, explains the scope of the change, and preserves the original conclusion. A correction does not erase earlier observations that were accurately attributed at the time. It changes the status of the conclusion and supplies the evidence or decision basis for the revised position. The incident coordinator updates the decision log with the correction's effective time and notifies the owners of any related customer, project, or vendor records.

## 4. Cross-region communication

Vortex Grid operates teams in North America, Europe, and Asia-Pacific. Meeting invitations, maintenance windows, and escalation deadlines must include an explicit timezone or an unambiguous UTC time. A local time may be included for convenience but does not replace the stated timezone. Recurring events must say whether their local time follows daylight-saving changes. If a calendar event is cancelled or rescheduled, the organizer must issue a cancellation or update rather than relying on a chat message alone.

During an active incident, the incident coordinator identifies the next decision time in UTC and records who is accountable for the update. A team member receiving a handoff is responsible for acknowledging the handoff in the relevant channel. Silence, an emoji reaction, or an unquoted reference to "the usual window" is not a substitute for a confirmed schedule. This requirement is particularly important when field teams and engineering teams are working across different local business days.

## 5. Vendor and customer records

Procurement and finance records must identify a supplier by its legal name and vendor identifier, not solely by a short name. If two suppliers use similar trading names, the buyer must preserve the distinction in purchase orders, invoices, approval notes, and reconciliation tables. A technical component description may be similar across suppliers without making the suppliers interchangeable. Questions about a charge, shipment, or part must be resolved against the specific record identifier and supplier identity.

Customer communications must distinguish customer-reported conditions from Vortex Grid findings. A support agent may describe an investigation and its next action, but may not state that a supplier or internal team caused a condition until the approved incident conclusion authorizes that statement. Legal, compliance, and customer operations review communications that include an admission of responsibility, contractual remedy, or regulatory notification.

## 6. Concurrent and unrelated matters

Two or more incidents, reviews, or supplier examinations may be open at the same time. Each keeps its own reference, coordinator, evidence, and conclusion. A record that mentions one matter must not be filed as evidence in another, and a control that was exercised during one matter is not thereby demonstrated for the other. Where a single export, calendar, register, or channel necessarily contains entries from more than one matter, the export must make the boundary legible: an identifier on every row, and a stated scope for the export as a whole.

Similarity is not connection. A shared customer site, a shared supplier short name, a shared reviewer, or a shared week does not create a relationship between two matters. The person who believes two matters are connected must record the specific evidence that connects them, name the records concerned, and obtain the agreement of both coordinators before either conclusion is written as though it covers the other. Absent that evidence, a summary that discusses both must present them separately, and must not compute a figure, trend, or rate that spans the two.

The reverse error is also prohibited. A team may not open a second reference to escape an inconvenient finding in the first, and may not close a matter by asserting that its remaining questions belong to some other review. Where a question is genuinely transferred between records, the transferring record states what was transferred, to which reference, and on whose authority, and the receiving record acknowledges it.

## 7. Accountability and exceptions

Team leaders train staff on this policy and review records for adequate attribution, time references, and correction history. The Records and Compliance group may audit whether a material incident has an initial report, decision log, final review, and customer communication trail. An exception must be approved in writing by the policy owner, state its duration and scope, and be attached to the affected record. An exception cannot authorize deletion of an original incident finding or substitution of an unattributed summary for a source record.

This policy takes effect on the date above. Earlier templates remain historical references only; new records must use the revision and handling rules stated here.