Dear [MANAGER],

I’m requesting approval to undertake *Mastering Embedded Cybersecurity*, an on-demand masterclass designed specifically for medical device developers. Courses are offered virtually and are at-your-own pace, so I’ll be able to schedule my training around our business milestones.

I’m interested in this training because the FDA and other regulators have released guidances on cybersecurity for medical devices, with more regulation under consideration in key markets worldwide. These publications clarify that new and even “substantially equivalent” device submissions must include a cybersecurity plan in order to be considered for approval. As we bring new devices to market, it is imperative that we have a cybersecurity plan for them. According to McKinsey & Company, [product recalls cost medical device manufacturers an average of $2 million per recall](https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/operations/pdfs/why_quality_should_be_on_medical_device_ceo_agenda.pdf), plus associated market share losses and drops in stock price. A quick search on the [FDA’s device recall database](https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm) shows that cybersecurity-related recalls are trending sharply upward. I don’t want our company to ever be part of those statistics.

The market is full of cybersecurity training. However, in my research I’ve found that most of these courses do not address the embedded products that we are developing. They focus on IT and network cybersecurity – the infrastructure surrounding the device – rather than on designing the device itself to be secure, even when the other devices in its network aren’t.

The embedded medical cybersecurity courses from Velentium are based on the bestselling engineering textbook [*Medical Device Cybersecurity for Engineers and Manufacturers*](https://www.amazon.com/Medical-Device-Cybersecurity-Engineers-Manufacturers/dp/1630818151/) and are taught by one of its principal authors, [Christopher Gates](https://www.velentium.com/leadership-bio#scrollid4). Each course includes theoretical instruction, hands-on exercises, and traceability and documentation training, followed by a robust certification exam. This approach provides us the certainty of knowing that we are on the right track with our cybersecurity development. After passing the final exam, I will receive a professional embedded cybersecurity certification.

Embedded cybersecurity experts are in high demand, due to [a global skills shortage that has been widening year by year](https://www.iso.org/news/ref2655.html). Qualified consultants charge in excess of $300/hour. I believe that by investing in this training ourselves, we can learn to do much more on our own and make embedded cybersecurity a key differentiator for our company at a significantly lower cost than hiring outside support.

The baseline cost for the masterclass is $7,995 per person for the first year, with an optional $1,495 per year for continuing education to maintain the certification. (If desired, we could save up to 20% with a multi-license training package for key personnel from our engineering, developer, R&D, quality & regulatory, and manufacturing teams).

I believe this is a good move for our company and hope that you agree! Please let me know if you need more information.

Thank you for considering this request.

[Your Name]